HP StorageWorks
8/20q Fibre Channel Switch installation and reference guide

8/20q Fibre Channel Switch installation and reference guide

Contents

About this guide

This guide provides information about:

- Becoming acquainted with the switch features and capabilities
- Planning a fabric including devices, device access, performance, multiple switch fabrics, switch services, fabric security, and fabric management.
- Installing and configuring an HP StorageWorks 8/20q Fibre Channel Switch
- Diagnosing and troubleshooting switch problems
-

Intended audience

This manual introduces users to the switch and explains its installation and service. It is intended for users who are responsible for installing and servicing network equipment.

Related documentation

In addition to this guide, please refer to other documents for this product:

- *HP StorageWorks 8/20q Fibre Channel Switch quick start installation instructions*
- *HP StorageWorks 8Gb Simple SAN Connection Kit quick start instructions*
- *HP StorageWorks 8/20q Fibre Channel Switch Rack Mount Kit quick start installation instructions*
- *HP StorageWorks 8Gb Simple SAN Connection Kit cabling guide*
- *HP StorageWorks 8/20q Fibre Channel Switch QuickTools switch management user guide*
- *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*
- *HP StorageWorks 8/20q Fibre Channel Switch command line interface quick reference guide*
- *HP StorageWorks Simple SAN Connection Manager user guide*
- *HP StorageWorks 8/20q Fibre Channel Switch event message reference guide*
- *HP StorageWorks 8/20q Fibre Channel Switch Simple Network Management Protocol reference guide*
- *HP StorageWorks 8/20q Fibre Channel Switch CIM Agent reference guide*

For the latest product information, including firmware, documentation, and supported SAN configurations, visit the following HP web site: http://www.hp.com/go/8Gb-SSC.

Document conventions and symbols

Table 1 Document conventions

Convention	Element
Medium blue text: Figure 1	Cross-reference links and e-mail addresses
Medium blue, underlined text (http://www.hp.com)	Web site addresses
Bold font	• Keys that are pressed • Text typed into a GUI element, such as into a box • GUI elements that are clicked or selected, such as menu and list items, buttons, and check boxes
Italics font	Text emphasis
`Monospace font`	• File and directory names • System output • Code • Commands, their arguments, and argument values
`Monospace, italic font`	• Code variables • Command-line variables
`Monospace, bold font`	Emphasis of monospace text, including file and directory names, system output, code, and text typed at the command line

⚠ **WARNING!**   Indicates that failure to follow directions could result in bodily harm or death.

△ **CAUTION:**   Indicates that failure to follow directions could result in damage to equipment or data.

📝 **IMPORTANT:**   Provides clarifying information or specific instructions.

📝 **NOTE:**   Provides additional information.

🔅 **TIP:**   Provides helpful hints and shortcuts.

Rack stability

⚠ WARNING!   To reduce the risk of personal injury or damage to equipment:
- Extend leveling jacks to the floor.
- Ensure that the full weight of the rack rests on the leveling jacks.
- Install stabilizing feet on the rack.
- In multiple-rack installations, secure racks together.
- Extend only one rack component at a time. Racks may become unstable if more than one component is extended.

HP technical support

Telephone numbers for worldwide technical support are listed on the HP support web site: http://www.hp.com/support/.

Collect the following information before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

Customer self repair

HP customer self repair (CSR) programs allow you to repair your StorageWorks product. If a CSR part needs replacing, HP ships the part directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your HP authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider. For North America, see the CSR website:

http://www.hp.com/go/selfrepair

This product has no customer replaceable components.

Product warranties

For information about HP StorageWorks product warranties, see the warranty information website:

http://www.hp.com/go/storagewarranty

Subscription service

HP strongly recommends that customers sign up online using the Subscriber's choice web site: http://www.hp.com/go/e-updates.

- Subscribing to this service provides you with e-mail updates on the latest product enhancements, newest versions of drivers, and firmware documentation updates as well as instant access to numerous other product resources.
- After signing up, you can quickly locate your products by selecting **Business support** and then **Storage** under Product Category.

HP web sites

For other product information, see the following HP web sites:

- http://www.hp.com
- http://www.hp.com/go/storage
- http://www.hp.com/support/
- http://www.docs.hp.com

Documentation feedback

HP welcomes your feedback.

To make comments and suggestions about product documentation, please send a message to storagedocs.feedback@hp.com. All submissions become the property of HP.

1 General description

The HP StorageWorks 8/20q Fibre Channel Switch (Figure 1) is a 20-port, 8-Gb/s switch with both Ethernet and serial management interfaces. This section describes the features and capabilities of the HP StorageWorks 8/20q Fibre Channel Switch and includes information about the following features:

- Switch LEDs and controls, page 12
- Fibre Channel ports, page 14
- Ethernet port, page 15
- Switch management, page 17

Fabrics are managed with the Command Line Interface (CLI) and the QuickTools web applet. You can also use the HP StorageWorks Simple SAN Connection Manager, which provides basic switch management functions, such as IP address configuration, and limited control of zoning.

- For more information about the CLI, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.
- For information about QuickTools, see the *HP StorageWorks 8/20q Fibre Channel Switch QuickTools switch management user guide*.
- For information about Simple SAN Connection Manager, see the *HP StorageWorks Simple SAN Connection Manager user guide*.
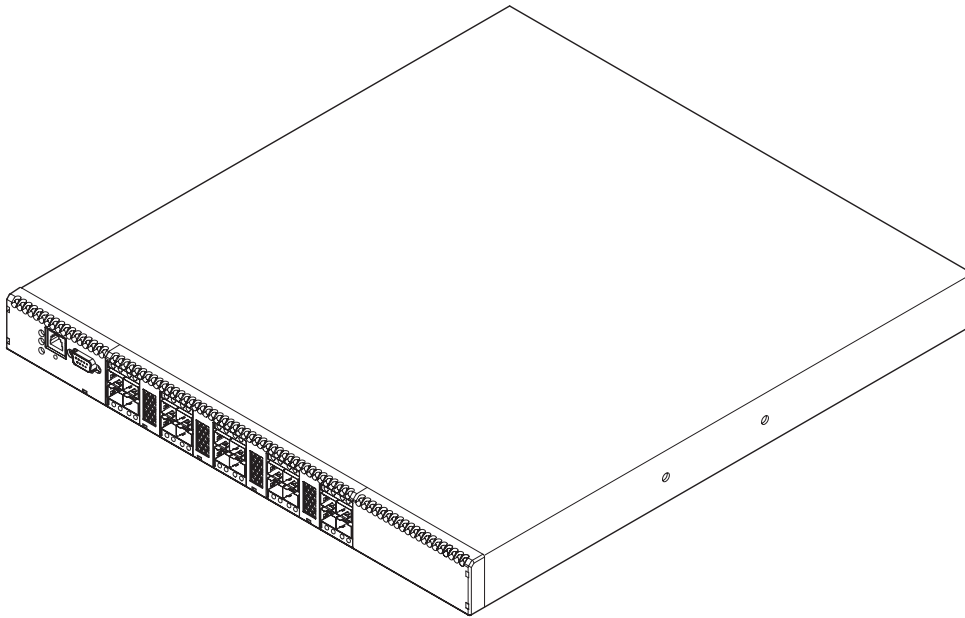
Figure 1 8/20q Fibre Channel Switch

Switch LEDs and controls

The switch LEDs provide information about the switch's operational status. These LEDS include the Input Power LED (green), Heartbeat LED (green), and the System Fault LED (amber) (Figure 2). For information about port LEDs, see "Port LEDs" on page 14. The Maintenance button (Figure 2) is the only switch control. It is used to reset a switch or to recover a disabled switch. To apply power to the switch, plug the power cord into the switch AC power receptacle, located on the back of the switch, and into a 100–240 VAC power source.
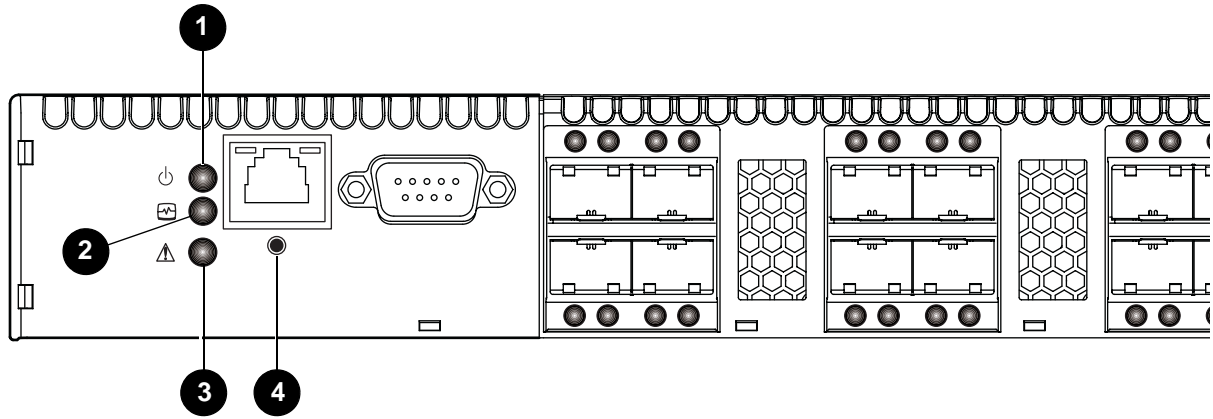
| 1 | Input Power LED (green) | 2 | Heartbeat LED (green) |
| 3 | System Fault LED (amber) | 4 | Maintenance button |

Figure 2 Switch LEDs and controls

Input power LED (green)

The Input Power LED indicates the voltage status at the switch logic circuitry. During normal operation, this LED illuminates to indicate that the switch logic circuitry is receiving the proper DC voltages. When the switch is in maintenance mode, this LED is extinguished.

Heartbeat LED (green)

The Heartbeat LED indicates the status of the internal switch processor and the results of the POST. Following a normal power-up, the Heartbeat LED blinks about once per second to indicate that the switch passed the POST and that the internal switch processor is running. In maintenance mode, the Heartbeat LED illuminates continuously. For more information, see "Heartbeat LED blink patterns" on page 42.

System fault LED (amber)

The System Fault LED illuminates to indicate that a fault exists in the switch firmware or hardware. Fault conditions include POST errors, over-temperature conditions, and power supply malfunctions. The Heartbeat LED shows a blink code for POST errors and over-temperature conditions. For more information, see "Heartbeat LED blink patterns" on page 42.

Maintenance button

The Maintenance button (Figure 2) is a dual-function momentary switch on the front panel. Its purpose is to reset the switch or to place the switch in maintenance mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes when flash memory or the resident configuration file is corrupted. For more information, see "Recovering a switch using maintenance mode" on page 46.

Resetting a switch

To reset the switch, press and hold the Maintenance button with a pointed tool for less than 2 seconds. The switch will respond as follows:

1. All the switch LEDs will illuminate except the System Fault LED.
2. After approximately 1 minute, the power-on self test (POST) begins, extinguishing the Heartbeat LED.
3. When the POST is complete, the Input Power LED is illuminated and the Heartbeat LED is flashing once per second.

Placing the switch in maintenance mode

To place the switch in maintenance mode:

1. Isolate the switch from the fabric.
2. Press and hold the Maintenance button with a pointed tool for a few seconds until only the Heartbeat LED (Figure 2) is illuminated. Continue holding the maintenance button until the Heartbeat LED goes off, then release the button. The Heartbeat LED illuminates continuously while the switch is in maintenance mode.

To exit maintenance mode and return to normal operation, press and release the Maintenance button momentarily to reset the switch.

Fibre Channel ports

The 8/20q Fibre Channel Switch has twenty Fibre Channel ports. Ports are numbered 0–19 (Figure 3). Each of the ports is served by a Small Form-Factor Pluggable (SFP+) transceiver and is capable of 8-Gb/s, 4-Gb/s, or 2-Gb/s transmission. SFPs are hot-pluggable. User ports can self-discover both the port type and transmission speed when connected to devices or other switches. The port LEDs are located above ports 0–9 and below ports 10–19, and provide port login and activity status information.
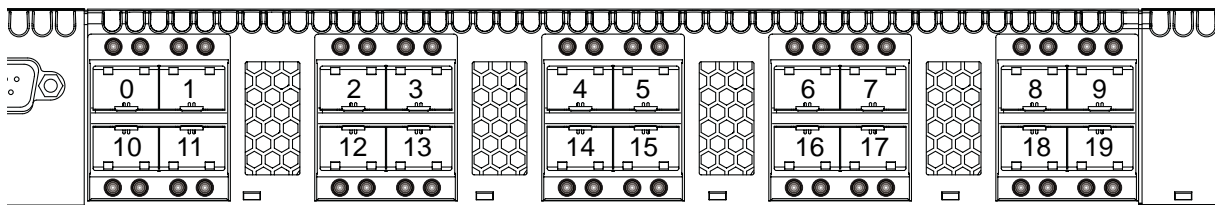
Figure 3 Fibre Channel ports

The 8/20q Fibre Channel Switch comes from the factory as an 8- or 16-port switch, enabling ports 0–7 or 0–15 respectively. You can enable additional ports up to the 20-port maximum using the HP StorageWorks 8/20q 4-port Upgrade License. For more information, see "Installing feature license keys" on page 40.

Port LEDs

Each port has its own Logged-in LED (green) and Activity LED (green) (Figure 4).
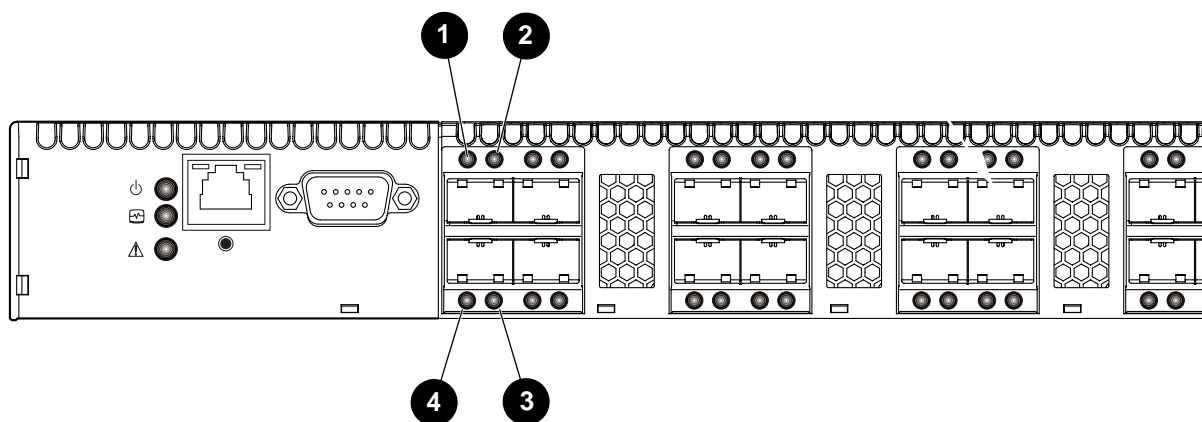
1	Logged-in LED (port 0)	2	Activity LED (port 0)
3	Activity LED (port 10)	4	Logged-in LED (port 10)

Figure 4 Port LEDs

Port Logged-in LED (green)

The Logged-in LED indicates the logged-in or initialization status of the connected devices. After successful completion of the POST, the switch extinguishes all Logged-in LEDs. Following a successful port login, the switch illuminates the corresponding logged-in LED. This shows that the port is properly connected and able to communicate with its attached devices. The Logged-in LED remains illuminated as long as the port is initialized or logged in. If the port connection is broken or an error occurs that disables the port, the Logged-in LED is extinguished. For more information, see "Logged-in LED indications" on page 44.

Port Activity LED (green)

The Activity LED indicates that data is passing through the port. Each frame that the port transmits or receives illuminates this LED for 50 milliseconds. This makes it possible to observe the transmission of a single frame.

Transceivers

The 8/20q Fibre Channel Switch supports SFP+ optical transceivers for the Fibre Channel ports. A transceiver converts electrical signals to and from optical laser signals to transmit and receive data. Duplex fiber optic cables plug into the transceivers which then connect to the devices. A port is capable of transmitting at 8 Gb/s, 4 Gb/s, or 2 Gb/s; however, the transceiver must also be capable of delivering at this rate.

The SFP+ transceivers are hot-pluggable. This means that you can remove or install a transceiver while the switch is operating without harming the switch or the transceiver. However, communication with the connected device will be interrupted. For information about installing and removing SFP+ optical transceivers, see "Install the transceivers" on page 33.

Port types

The 8/20q Fibre Channel Switch supports generic ports (G_Port, GL_Port), fabric ports (F_Port, FL_Port), and expansion ports (E_Port). Switches come from the factory with all Fibre Channel ports configured as GL_Ports. Generic, fabric, and expansion ports function as follows:

- A GL_Port self-configures as an FL_Port when connected to a loop device, as an F_Port when connected to a single device, or as an E_Port when connected to another switch. If the device is a single device on a loop, the GL_Port will attempt to configure first as an F_Port, then if that fails, as an FL_Port.
- A G_Port self-configures as an F_Port when connected to a single device, or as an E_Port when connected to another switch.
- An FL_Port supports a loop of up to 126 devices. An FL_Port can also configure itself during the fabric login process as an F_Port when connected to a single device (N_Port).
- An F_Port supports a single device.
- E_Ports enable you to expand the fabric by connecting 8/20q Fibre Channel Switches. The 8/20q Fibre Channel Switch self-discovers all inter-switch connections. For more information, see "Multiple switch fabrics" on page 21.

Ethernet port

The Ethernet port is an RJ-45 connector that provides a connection to a workstation through a 10/100 Base-T Ethernet cable (Figure 5). A workstation can be a Windows or a Linux server that is used to configure and manage the switch fabric. An Ethernet connection to the switch is required to manage the switch using the CLI, QuickTools, Simple SAN Connection Manager, or Simple Network Management Protocol (SNMP).

The Ethernet port has two LEDs: the Link Status LED (green) and the Activity LED (green). The Link Status LED illuminates continuously when an Ethernet connection has been established. The Activity LED illuminates when data is being transmitted or received over the Ethernet connection.
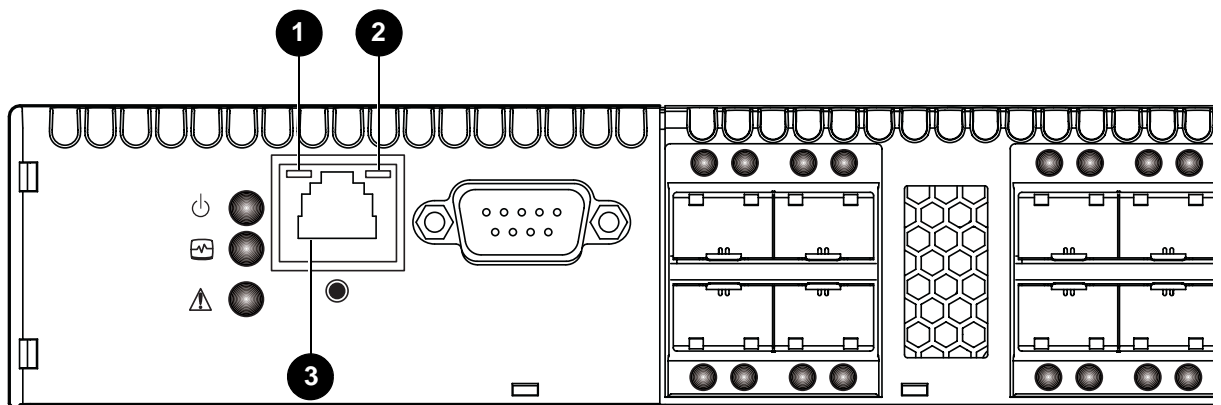
1	Activity LED	**2**	Link status LED
3	RJ-45 Ethernet port		

Figure 5 Ethernet port

Serial port

The 8/20q Fibre Channel Switch is equipped with an RS-232 serial port for maintenance purposes (Figure 6). You can manage the switch through the serial port using the CLI.
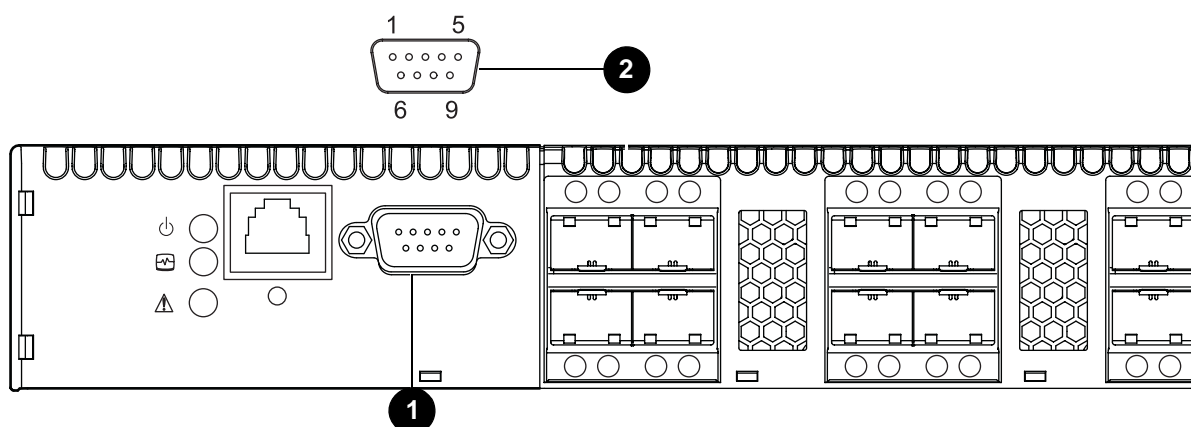
| 1 | Serial port | 2 | RS-232 connnector pin identification |

Figure 6 Serial port and pin identification

The serial port connector requires a null-modem F/F DB9 cable. The pins on the switch RS-232 connector (Figure 6) are identified in Table 2. For information about connecting the workstation through the serial port, see "Connect the management station or workstation to the switch" on page 35.

Table 2 Serial port pin identification

Pin Number	Description	Referrred to as
1	Carrier Detect	DCD
2	Receive Data	RxD
3	Transmit Data (TxD)	TxD
4	Data Terminal Ready (DTR)	DTR
5	Signal Ground (GND)	GND
6	Data Set Ready (DSR)	DSR
7	Request to Send (RTS)	RTS
8	Clear to Send (CTS)	CTS
9	Ring Indicator (RI)	RI

Power supply and fans

The switch has a single power supply that converts 100–240 VAC to DC voltages for the various switch circuits. Four internal fans provide cooling. The switch monitors internal air temperature, and therefore does not monitor or report fan operational status. Air flow is front-to-back. To energize the switch, plug the power cord into the switch AC receptacle (located on the back of the switch) and into a 100–240 VAC power source.

Switch management

The switch supports the following management tools and protocols:

QuickTools web applet

QuickTools is a browser-based graphical user interface (GUI) that provides switch management capabilties beyond those of Simple SAN Connection Manager. You run QuickTools by opening the switch IP address with an internet browser on your workstation. See the *HP StorageWorks 8/20q Fibre Channel Switch QuickTools switch management user guide*. QuickTools provides the following management features:

- Faceplate device management
- Switch and port statistics
- Configuration wizard
- Zoning administration
- Fabric tree for fabric management
- User account configuration
- Switch and fabric events
- Operational and environmental statistics
- Global device nicknames
- Inband management of other switches in the fabric
- Online help

Simple SAN Connection Manager

HP StorageWorks Simple SAN Connection Manager is a GUI-based management application for HP StorageWorks that runs on a workstation known as the management station. It provides basic automated configuration and management of switches, HBAs, and storage devices.

Command line interface

The command line interface (CLI) provides monitoring and configuration functions by which the administrator can manage the fabric and its switches. The CLI is available over an Ethernet connection or a serial connection. For more information, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

Simple Network Management Protocol

SNMP provides monitoring and trap functions for the fabric. The switch firmware supports SNMP versions 1 and 2, the Fibre Alliance Management Information Base (FA-MIB) version 4.0, and the Fabric Element Management Information Base (FE-MIB) RFC 2837. Traps can be formatted using SNMP version 1 or 2. For more information, see the *HP StorageWorks 8/20q Fibre Channel Switch Simple Network Management Protocol reference guide*.

Storage Management Initiative–Specification (SMI-S)

SMI-S provides for the management of the switch through third-party applications that use the SMI-S. For more information, see the *HP StorageWorks 8/20q Fibre Channel Switch CIM Agent reference guide*.

File transfer protocols

FTP and TFTP provide the command line interface for exchanging files between the switch and the workstation. These files include firmware image files, configuration files, and log files. For more information about FTP and TFTP, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

2 Planning

Consider the following when planning a fabric:

Devices

When planning a fabric, consider the number of devices and the anticipated demand. This will determine the number of ports that are needed and in turn the number of switches.

Consider the transmission speeds of your HBAs and SFPs. The switch supports 2-Gb/s, 4-Gb/s, and 8-Gb/s transmission speeds.

Consider also the distribution of targets and initiators. An F_Port supports a single device. An FL_Port can support up to 126 devices in an arbitrated loop.

Device access

Consider device access needs within the fabric. Access is controlled by the use of zoning. Some zoning strategies include the following:

- Separate devices by operating system.
- Separate devices that have no need to communicate with other devices in the fabric or have classified data.
- Separate devices into department, administrative, or other functional group.
- Reserve a path and its bandwidth from one port to another.

Zoning divides the fabric for purposes of controlling discovery and inbound traffic. A zone is a named group of ports or devices. Members of the same zone can communicate with each other and transmit outside the zone, but cannot receive inbound traffic from outside the zone. Zoning is hardware-enforced only when a port/device is a member of no more than eight zones whose combined membership does not exceed 64. If this condition is not satisfied, that port behaves as a soft zone member. You can assign ports/devices to a zone individually or as a group by creating an alias.

A zone can be a component of more than one zone set. Several zone sets can be defined for a fabric, but only one zone set can be active at one time. The active zone set determines the current fabric zoning.

A zoning database is maintained on each switch. Table 3 describes the zoning database limits, excluding the active zone set.

Table 3 Zoning database limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256).
MaxZones	Maximum number of zones (2,000).
MaxAliases	Maximum number of aliases (2,500).
MaxTotalMembers	Maximum number of zone and alias members (10,000) that can be stored in the zoning database. Each instance of a zone member or alias member counts toward this maximum.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (2,000), excluding the orphan zone set. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2,000).
MaxMembersPerAlias	Maximum number of members in an alias (2,000)

Performance

The 8/20q Fibre Channel Switch supports class 2 and class 3 Fibre Channel service at transmission rates of 8-Gb/s with a maximum frame size of 2,148 bytes. Related performance characteristics include the following:

- Distance, page 20
- Bandwidth, page 20
- Latency, page 21

Distance

Consider the physical distribution of devices and switches in the fabric. Choose SFP transceivers that are compatible with the cable type, distance, Fibre Channel revision level, and the device host bus adapter. For more information about cable types and transceivers, see "Technical specifications" on page 55.

Each Fibre Channel port is supported by a data buffer with a 16 credit capacity; that is, 16 maximum sized frames. For fibre optic cables, this enables full bandwidth over approximately 3 kilometers at 8 Gb/s (4.8 credits/km).

Bandwidth

Bandwidth is a measure of the volume of data that can be transmitted at a given transmission rate. A Fibre Channel port can transmit or receive at nominal rates of 8 Gb/s, 4 Gb/s, or 2 Gb/s depending on the device to which it is connected. This corresponds to full duplex bandwidth values of 1,700 MB, 850 MB, and 424 MB respectively. Multiple source ports can transmit to the same destination port if the destination bandwidth is greater than or equal to the combined source bandwidth. For example, two 4 Gb/s source ports can transmit to one 8 Gb/s destination port. Similarly, one source port can feed multiple destination ports if the combined destination bandwidth is greater than or equal to the source bandwidth.

In multiple switch fabrics, each link contributes up to 1,700 MB of bandwidth between those switches, depending on the speed of the link. When additional bandwidth is needed between devices, increase the number of links between the connecting switches. The switch guarantees in-order delivery with any number of links.

Latency

Latency is a measure of how fast a frame travels through a switch from one port to another. The factors that affect latency include transmission rate and the source/destination port relationship (Table 4).

Table 4 Port-to-port latency

	Destination Rate			
	Gbps	2	4	8
Source Rate	2	< 0.6 μsec	< 0.7 μsec[1]	< 0.6 μsec[1]
	4	< 0.4 μsec	< 0.3 μsec	< 0.4 μsec[1]
	8	< 0.3 μsec	< 0.2 μsec	< 0.2 μsec

1. Based on minimum frame size of 36 bytes. Latency increases for larger frame sizes.

Feature licenses

License keys provide a way to expand the capabilities of your switch and fabric as your needs grow. The HP StorageWorks 8/20q 4-port Upgrade License activates additional Fibre Channel ports to 12, 16, or 20 ports. Applying a license key is not disruptive, nor does it require a switch reset. To order a license key, contact your switch distributor or your authorized reseller. For more information, see "Installing feature license keys" on page 40.

Multiple switch fabrics

By connecting switches to one another, you can expand the number of available ports for devices. Each switch in the fabric is identified by a unique domain ID, and the fabric can automatically resolve domain ID conflicts. Because the Fibre Channel ports are self-configuring, you can connect 8/20q Fibre Channel Switches together in a wide variety of topologies. When planning your fabric, consider your topology and cabling requirements. For more information about Storage Area Network (SAN) connectivity, see the *SAN design reference guide* available at the HP website: http://www.hp.com/go/SANdesignguide.

Optimizing device performance

When choosing a topology for a multiple switch fabric, you should also consider the proximity of your server and storage devices and the performance requirements of your application. Storage applications such as video distribution, medical record storage/retrieval, or real-time data acquisition can have specific latency or bandwidth requirements.

The 8/20q Fibre Channel Switch provides the lowest latency of any product in its class. For information about latency, see "Performance" on page 20. However, the highest performance is achieved on Fibre Channel switches by keeping traffic within a single switch instead of relying on ISLs. Therefore, for optimal device performance, place devices on the same switch under the following conditions:

- Heavy I/O traffic between specific server and storage devices.
- Distinct speed mismatch between devices such as the following:
  - An 8-Gb/s server and a slower 2-Gb/s storage device
  - A high performance server and slow tape storage device

Domain ID, principal priority, and domain ID lock

The following switch configuration settings affect multiple switch fabrics:

- Domain ID
- Principal priority
- Domain ID lock

The domain ID is a unique number from 1–239 that identifies each switch in a fabric. The principal priority is a number (1–255) that determines the principal switch which manages domain ID assignments for the fabric. The switch with the highest principal priority (1 is high, 255 is low) becomes the principal switch. If the principal priority is the same for all switches in a fabric, the switch with the lowest Worldwide Name (WWN) becomes the principal switch.

The domain ID lock allows (False) or prevents (True) the reassignment of the domain ID on that switch. Switches come from the factory with the domain ID set to 1, the domain ID lock set to False, and the principal priority set to 254. For information about changing the default domain ID, domain ID lock, and principal priority parameters, see the `set config switch` command in the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain ID conflict occurs, the new switch will isolate as a separate fabric. You can remedy this by resetting the new switch or taking it offline then putting it back online. The principal switch will reassign the domain ID and the switch will join the fabric.

NOTE: Domain ID reassignment is not reflected in zoning that is defined by domain ID/port number pair or Fibre Channel address. You must reconfigure zones that are affected by domain ID reassignment. To prevent zoning definitions from becoming invalid under these conditions, lock the domain IDs. Domain ID reassignment has no effect on zone members defined by WWN.

Common topologies

For additional information about Storage Area Network (SAN) connectivity, see the *SAN design reference guide* available at the HP website: http://www.hp.com/go/SANdesignguide.

Switch services

You can configure your switch to suit the demands of your environment by enabling or disabling a variety of switch services. Familiarize yourself with the following switch services and determine which ones you need.

- **Telnet**: Provides for the management of the switch over a Telnet connection. Disabling this service is not recommended. The default is enabled.
- **Secure Shell (SSH)**: Provides for secure remote connections to the switch using SSH. Your workstation must also use an SSH client. The default is disabled.
- **GUI Management**: Provides for out-of-band management of the switch with Simple SAN Connection Manager, QuickTools, SNMP, and SMI-S. If this service is disabled, the switch can only be managed inband or through the serial port. The default is enabled.
- **Inband Management**: Provides for the management of the switch over an inter-switch link using Simple SAN Connection Manager, QuickTools, SNMP, or management server. If you disable inband management, you can no longer communicate with that switch by means other than an Ethernet or serial connection. The default is enabled.

- **Secure Socket Layer (SSL)**: Provides for secure SSL connections for the QuickTools web applet and SMI-S. This service must be enabled to authenticate users through a Remote Authenticaton Dial-in Service (RADIUS) server. To enable secure SSL connections, you must first synchronize the date and time on the switch and the workstation. Enabling SSL automatically creates a security certificate on the switch. The default is disabled.

> **NOTE:** Simple SAN Connection Manager version 1.0 does not support the SSL service. If SSL is enabled, you will be unable to manage the switch using this version of Simple SAN Connection Manager.

- **QuickTools web applet (EmbeddedGUI)**: Provides for access to the QuickTools web applet. QuickTools enables you to point at a switch with an internet browser and manage the switch through the browser. The default is enabled.
- **Simple Network Management Protocol (SNMP)**: Provides for the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). Security consists of a read community string and a write community string that serve as passwords that control read and write access to the switch. These strings are set at the factory to these well-known defaults and should be changed if SNMP is to be enabled. Otherwise, you risk unwanted access to the switch. The default is enabled.
- **Common Information Model (CIM)**: Provides for the management of the switch through third-party applications that use the Storage Management Initiative–Specification (SMI-S). The default is enabled.
- **File Transfer Protocol (FTP)**: Provides for transferring files rapidly between the workstation and the switch using FTP. The default is enabled.
- **Management Server (MS)**: Enables or disables the management of the switch through third-party applications that use FC-GS-3 Management Server. The default is disabled.
- **Call Home:**

> **IMPORTANT:** The Call Home service provides an e-mail notification capability for the switch. This service has no relationship with the HP Call Home feature, which notifies only HP services.

Provides for automated e-mail notification of switch status and operating conditions based on specified event severity levels. The default is enabled. The Call Home service requires an Ethernet connection to at least one Simple Mail Transfer Protocol (SMTP) server. You must configure the Call Home service to do the following:

- Enable primary and secondary SMTP servers and specify their IP addresses
- Specify contact information

Configure one or more Call Home profiles to specify e-mail recipients, message format, and the event severity level that will initiate a message.

Fabric security

An effective security profile begins with a security policy that states the requirements. A threat analysis is needed to define the plan of action, followed by an implementation that meets the security policy requirements. Internet portals, such as remote access and E-mail, usually present the greatest threats. Fabric security should also be considered in defining the security policy.

Most fabrics are located at a single site and are protected by physical security, such as key-code locked computer rooms. For these cases, security methods, such as user passwords for equipment and zoning for controlling device access, are satisfactory.

Fabric security is needed when security policy requirements are more demanding; for example, when fabrics span multiple locations and traditional physical protection is insufficient to protect the IT infrastructure. Another benefit of fabric security is that it creates a structure that helps prevent unintended changes to the fabric.

Fabric security consists of the following:

- Connection security, page 24
- User account security, page 24
- Port binding, page 25
- Device security, page 25

Connection security

Connection security provides an encrypted data path for switch management methods. The switch supports the Secure Shell (SSH) protocol for the command line interface and the Secure Socket Layer (SSL) protocol for management applications such as QuickTools and SMI-S. Use the CLI to configure SSH and SSL. For more information about SSH and SSL configuration, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

The SSL handshake process between the workstation and the switch involves the exchanging of certificates. These certificates contain the public and private keys that define the encryption. When the SSL service is enabled, a certificate is automatically created on the switch. The workstation validates the switch certificate by comparing the workstation date and time to the switch certificate creation date and time. For this reason, it is important to synchronize the workstation and switch with the same date, time, and time zone. The switch certificate is valid 24 hours before its creation date and 365 days after its creation date. If the certificate should become invalid, create a new certificate using the `create certificate` CLI command. For information about the `create certificate` CLI command, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

NOTE: Simple SAN Connection Manager version 1.0 does not support the SSL service. If SSL is enabled, you will be unable to manage the switch using this version of Simple SAN Connection Manager.

Consider your requirements for connection security: for the command line interface (SSH), management applications (SSL), or both. If an SSL connection security is required, also consider using the Network Time Protocol (NTP) to synchronize workstations and switches.

User account security

User account security consists of the administration of account names, passwords, expiration date, and authority level. If an account has Admin authority, all management tasks can be performed by that account in the CLI, QuickTools, and Simple SAN Connection Manager. Otherwise only monitoring tasks are available. The default account name, Admin, is the only account that can create or add account names and change passwords of other accounts. All users can change their own passwords. Account names and passwords are always required when connecting to a switch.

Authentication of the user account and password can be performed locally using the switch's user account database or it can be done remotely using a RADIUS server such as Microsoft RADIUS. Authenticating user logins on a RADIUS server requires a secure management connection to the switch. For information about securing the management connection, see "Connection security" on page 24. A RADIUS server can also be used to authenticate devices and other switches as described in "Device security" on page 25.

Consider your management needs and determine the number of user accounts, their authority needs, and expiration dates. Also consider the advantages of centralizing user administration and authentication on a RADIUS server. Use the CLI to configure RADIUS servers. For more informaton about RADIUS server configuration, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

NOTE: If the same user account exists on a switch and its RADIUS server, that user can login with either password, but the authority and account expiration will always come from the switch database.

Port binding

Port binding provides authorization for a list of up to 32 switch and device WWNs that are permitted to log in to a particular switch port. Switches or devices that are not among the 32 are refused access to the port. Consider what ports to secure and the set of switches and devices that are permitted to log in to those ports. Use the CLI to configure port binding. For more informaton about port binding configuration, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

Device security

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or devices issuing management server commands. Device security is configured through the use of security sets and groups. Use the CLI to configure device security. For more information about device security configuration, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS).

A security set is a set of up to three groups with no more than one of each group type. The security configuration is made up of all security sets on the switch. The security database has the following limits:

- Maximum number of security sets is 4.
- Maximum number of groups is 16.
- Maximum number of members in a group is 1,000.
- Maximum total number of group members is 1,000.

In addition to authorization, the switch can be configured to require authentication to validate the identity of the connecting switch, device, or host. Authentication can be performed locally using the switch's security database, or remotely using a RADIUS server such as Microsoft RADIUS. With a RADIUS server, the security database for the entire fabric resides on the server. In this way, the security database can be managed centrally, rather than on each switch. You can configure up to five RADIUS servers to provide failover.

You can configure the RADIUS server to authenticate just the switch or both the switch and the initiator device if the device supports authentication. When using a RADIUS server, every switch in the fabric must have a network connection. A RADIUS server can also be configured to authenticate user accounts as described in "User account security" on page 24. A secure connection is required to authenticate user logins with a RADIUS server. For more information, see "Connection security" on page 24.

Consider the devices, switches, and management agents and evaluate the need for authorization and authentication. Also consider whether the security database is to be distributed on the switches or centralized on a RADIUS server and how many servers to configure. Use the CLI to configure RADIUS servers. For more information about RADIUS server configuration, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

Fabric management

The Simple SAN Connection Manager application is a GUI-based management application for HP StorageWorks that runs on the management station. It provides basic automated configuration and management of switches, HBAs, and storage devices. Switch management functions include IP address configuration and limited control of zoning.

The browser-based application, QuickTools, and the CLI reside in the switch firmware and provide for the management of individual switches in a single fabric.

Consider how many fabrics and switches will be managed, how many workstations are needed, and whether the fabrics will be managed with Simple SAN Connection Manager, QuickTools, or the CLI.

A switch supports a combined maximum of 19 logins, which are reserved as follows:

- 4 logins or sessions for internal applications, such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for Simple SAN Connection Manager inband and out-of-band logins, QuickTools logins, and Telnet logins.

Additional logins will be refused.

3 Installation

This section describes how to install and configure the switch. The following topics are covered:

Site requirements

Consider the following items when installing an 8/20q Fibre Channel Switch:

Management Station and Workstation requirements

The management station requirements for Simple SAN Connection Manager are described in Table 5. Workstation requirements for QuickTools are described in Table 6.

Table 5   Management station requirements for Simple SAN Connection Manager

Operating System	Windows Server 2003 R2 SP2
Memory	512 MB
Disk Space	150 MB per installation
Processor	2 GHz or faster
Internet browser	Microsoft Internet Explorer 5.0 or later
	Netscape Navigator 6.0 and later
	Mozilla 1.5 and later
	Firefox 1.0 and later
	Java Runtime Environment 1.5 or higher
Hardware	CD ROM drive
	RJ-45 Ethernet port
	PCI-e slots for the HP StorageWorks PCI-e FC HBA

Table 6 Workstation requirements for QuickTools

Operating systems	Windows 2003 and XP SP1/SP2
	Red Hat Enterprise Linux 3, 4
	SUSE Linux Enterprise Server 9 and 10
Memory	512 MB
Processor	2 GHz or faster
Internet Browser	Microsoft Internet Explorer 5.0 or later
	Netscape Navigator 6.0 and later
	Mozilla 1.5 and later
	Firefox 1.0 and later
	Java Runtime Environment 1.4.2 or higher[1]
Hardware	RJ-45 Ethernet port

1. You must disable caching of temporary files and applets in Java to prevent conflicts with past or future versions of QuickTools. Furthermore, you may need to disable caching again after upgrading Java.

Telnet workstations require an RJ-45 Ethernet port or an RS-232 serial port and an operating system with a Telnet client.

Switch power requirements

Power requirements are 1 Amp at 100 VAC or 0.5 A at 240 VAC.

Environmental conditions

Consider the factors that affect the climate in your facility such as equipment heat dissipation and ventilation. The switch requires the following operating conditions:

- Operating temperature range: 0°–40°C (0°–104°F)
- Relative humidity: 15–80%, non-condensing

Installing a switch

Unpack the switch and accessories. The 8/20q Fibre Channel Switch product is shipped with the following components

- One *Read-Me-First* document
- One *End User License Agreement (EULA)*
- *HP StorageWorks 8/20q Fibre Channel Switch Rack-Mount Kit quick start installation instructions*
- *HP StorageWorks 8/20q Fibre Channel Switch quick start installation instructions*
- One HP StorageWorks Simple SAN Connection Manager software CD
- One HP StorageWorks 8/20q Fibre Channel Switch
- One HP StorageWorks 8/20q Fibre Channel Switch Rack-Mount Kit
- One standard power cord
- One HP Power Distribution Unit (PDU) power cable
- One serial cable
- Four ahesive rubber feet

For the latest product information, including firmware, documentation, and supported SAN configurations, visit the following HP web site: http://www.hp.com/go/8Gb-SSC.

Installing a 8/20q Fibre Channel Switch involves the following steps:

Mount the switch

The switch can be placed on a flat surface and stacked, or mounted in a 19" Electronics Industries Association (EIA) rack. See "Weight and physical dimensions" on page 57 for weight and dimensional specifications. Adhesive rubber feet are provided for surface mounts only. Without the rubber feet, the switch occupies 1U of space in an EIA rack.

The rack mount kit is supported with the following HP custom racks only:

- HP 9000 Series Rack
- HP 10000 Series Rack
- HP 10000 G2 Series Rack

Before you begin

⚠ **WARNING!**   To reduce the risk of personal injury or damage to the equipment, ensure that:

- In single-rack installations, stabilizing feet are attached to the rack.
- In multiple-rack installations, racks are coupled together.
- Leveling jacks on the rack are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- Heavy items, such as uninterruptible power supplies and hard drive storage enclosures, are installed near the bottom of the rack.
- Similar components are installed next to each other in the rack. Because devices are of differing depths, this will facilitate maintenance and service tasks.
- Only one device in a rack is extended at a time. A rack may become unstable if more than one device is extended.

△ **CAUTION:**

- For proper airflow, the SFP+ media side (port side) of the device must face the front of the rack. Mounting the switch in this direction allows air to enter from the front of the rack (SFP-port side of switch) and exhaust through the back of the rack (power-supply side of switch). This prevents overheating, which may cause equipment in the rack to fail.
- Allow a minimum of 63.5 cm (25 in.) clearance in front of the rack to allow the doors to open fully, and 76.2 cm (30 in.) in back of the rack to allow for servicing and airflow.
- If the device is mounted in a closed rack or there are multiple rack-mounted devices, make sure that the operating temperature inside the rack enclosure does not exceed the maximum rated ambient temperature.
- Multiple rack-mounted devices connected to the same AC supply circuit may overload that circuit or the AC supply wiring. Consider the power source capacity and the total power usage of all switches on the circuit.
- Reliable grounding in the rack must be maintained.

Collect the required items

📝 **NOTE:** The rack mount kit installation requires one technician.

Locate the following items and set them aside:

- 8/20q Fibre Channel Switch
- 8/20q Fibre Channel Switch rack-mount kit
- Smaller items, such as screws, ship in plastic bags in the kit. See Table 7.
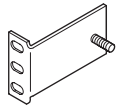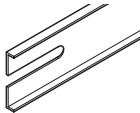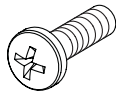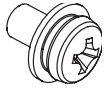
Required tools:

- #2 Phillips screwdriver
- 7/16-inch wrench

Verify the kit contents

Check the contents of the 8/20q Fibre Channel Switch rack mount kit shipping carton to verify that all required parts and hardware are available (Table 7).

Table 7   8/20q Fibre Channel Switch rack mount kit hardware

Item	Description
	Two (2) rear mounting brackets
	Two (2) switch rails
	One (1) filler panel (optional), see step 7.
	Ten (10) M6 machine screws
	Ten (10) M6 cage-nuts for square rack holes
	Ten (10) M6 cage-nuts for round rack holes
	Four (4) 10-32 x .375-inch screws with captive washers
	Two (2) 1/4-20 hex nuts with lock washers
	Two (2) 1/4-inch flat washers

Rack the switch

1. Remove and discard the four 10-32 screws from the sides of the switch.
2. Attach each rail to the switch using two 10-32 x .375-inch screws with captive washers (Figure 7). Make sure the slotted ends of the rails are on the power-supply side (not the SFP-port side) of the switch.
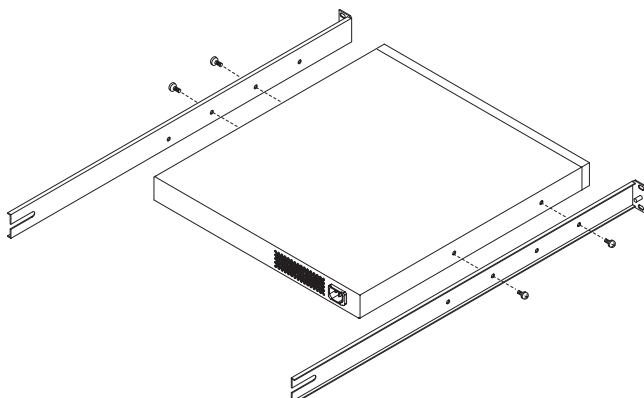
Figure 7 Attaching the rails to the switch

3. On the rack vertical posts, mark the holes that will be used by the rail flanges (three on each rear vertical post, two on each front vertical post). Then, from the inside of each vertical post, insert an M6 cage-nut for the rack you are using (square or round hole) into each marked hole (Figure 8).

   Fasten each rear mounting bracket to the marked holes, using two M6 machine screws.
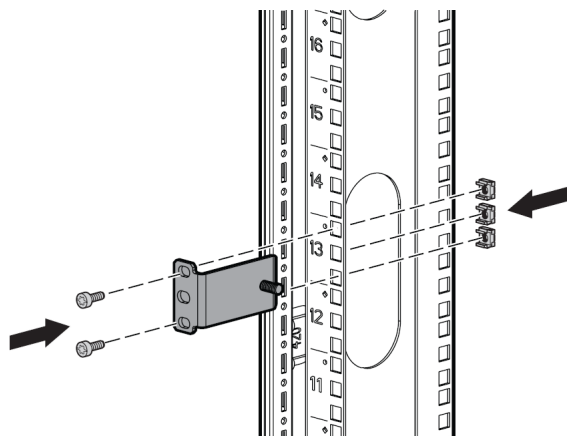
Figure 8 Installing the rear mounting brackets

4. Place the switch and rail assembly into the rack through the front, guiding the slotted-rail ends onto the threaded studs of the rear mounting brackets (Figure 9). Fit the posts on the front rail flanges in the holes between the two cage-nuts on each of the front vertical rack posts.
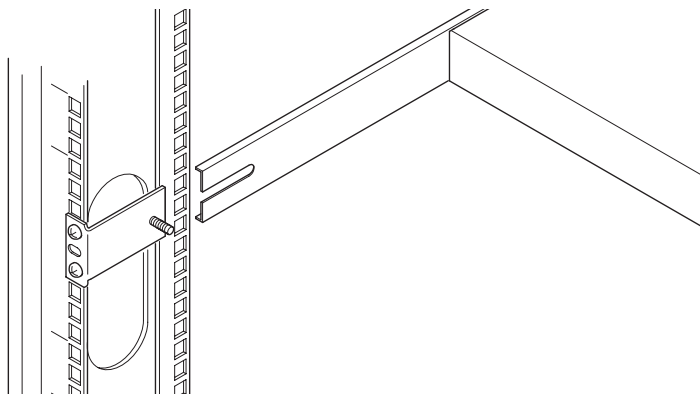
Figure 9 Installing the switch and rail assembly

5. Fasten each rail flange to the front of the rack using two M6 machine screws (Figure 10).
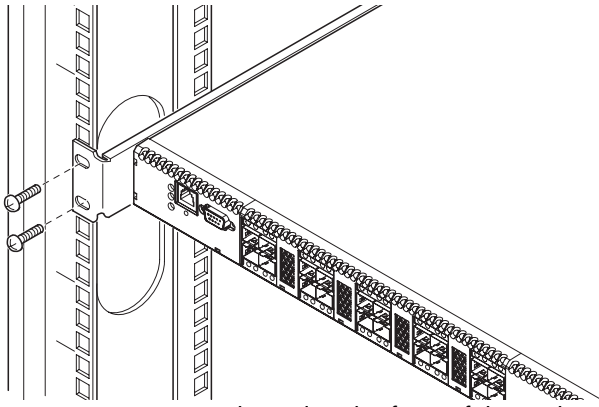
Figure 10 Fastening the rail to the front of the rack

6. Fasten each slotted-rail end to the rear mounting bracket using a flat washer and a 1/4-20 hex nut (Figure 11).
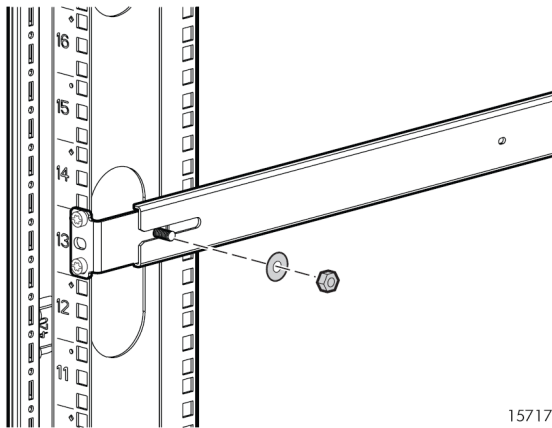
Figure 11 Fastening the rail to the rear mounting bracket

7. Optional: Fasten the filler panel to the rear mounting brackets with two M6 machine screws (Figure 12).
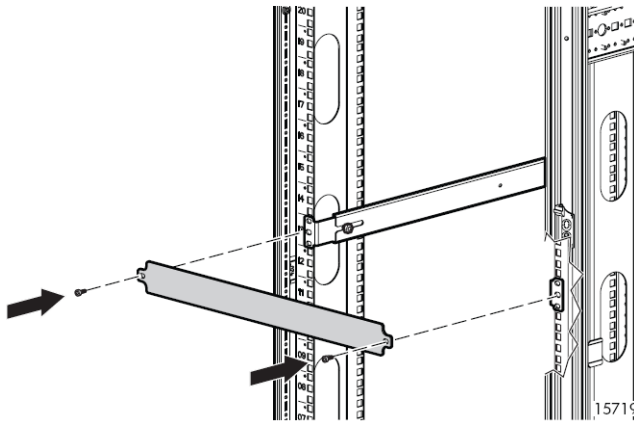
Figure 12 Installing the filler panel

Install the transceivers

A small form-factor pluggable (SFP) transceiver is required for each switch port that will be connected to a device or another switch. SFPs are not included with the switch. Only HP SFPs are supported for use in the switch. To install an SFP transceiver, insert the transceiver into any of the active switch ports and gently press until it snaps in place.

☼ **TIP:**   The transceiver will fit only one way. If the transceiver is not installed under gentle pressure, flip it over and try again.

A new switch has eight (ports 0–7) or sixteen (ports 0–15) active ports depending on the model. Additional ports can be activated with the HP StorageWorks 8/20q 4-port Upgrade License. For more information, see "Installing feature license keys" on page 40.

Configure the workstation

📝 **NOTE:**   If you plan to use Simple SAN Connection Manager or QuickTools to manage the switch, proceed to "Apply power to the switch" on page 34.

If you plan to use the CLI to configure and manage the switch, you must configure the workstation. This involves setting the workstation IP address for Ethernet connections, or configuring the workstation serial port.

Configuring the workstation IP address for Ethernet connections

The default IP address of a new switch is 10.0.0.1. To ensure that your workstation is configured to communicate with the 10.0.0 subnet:

- For a Windows workstation:
  a. Click **Start** then choose **Settings**>**Control Panel**>**Network and Dial-Up Connections**.
  b. Choose **Make New Connection**.
  c. Click the **Connect to a private network through the Internet** radio button, then click **Next**.
  d. Enter **10.0.0.253** for the IP address.
- For a Linux workstation, open a command window and enter the following command where *interface* is your interface name:

      ifconfig *interface* ipaddress 10.0.0.253 netmask 255.255.255.0 up

Configuring the workstation serial port

To configure the workstation serial port:

1. Connect a null modem F/F DB9 cable from a COM port on the workstation to the RS-232 serial port on the switch.
2. Configure the workstation serial port according to your platform:

   For a Windows workstation:
   a. Open the HyperTerminal application. Click **Start**, then select **Programs>Accessories> Communications>HyperTerminal**.
   b. Enter a name for the switch connection and choose an icon in the Connection Description window. Click **OK**.
   c. Enter the following COM Port settings in the COM Properties window, and click **OK**.
      - Bits per second: 9,600
      - Data Bits: 8
      - Parity: None
      - Stop Bits: 1
      - Flow Control: None

For a Linux workstation:

a. Set up minicom to use the serial port. Create or modify the `/etc/minirc.dfl` file with the following content.

```
pr portdev/ttyS0
pu minit
pu mreset
pu mhangup
```

b. Verify that all users have permission to run minicom. Review the `/etc/minicom.users` file and confirm that the line `ALL` exists or that there are specific user entries.

Apply power to the switch

⚠ **WARNING!**   This product is supplied with a 3-wire power cable and plug for the user's safety. Use this power cable in conjunction with a properly grounded outlet to avoid electrical shock. An electrical outlet that is not correctly wired could place hazardous voltage on metal parts of the switch. It is the responsibility of the customer to ensure that the outlet is correctly wired and grounded to prevent electrical shock.

You may require a different power cable in some countries because the plug on the cable supplied with the equipment will not fit your electrical outlet. In this case, you must supply your own power cable. The cable you use must meet the following requirements:

- For 125 Volt electrical service, the cable must be rated at 10 Amps and be approved by Underwriters Laboratories (UL) and Canadian Standards Association (CSA).
- For 250 Volt electrical service: The cable must be rated at 10 Amps, meet the requirements of H05VV-F, and be approved by Verband der Elektrotechnik (VDE), SEMKO, and DEMKO.

To power up a 8/20q Fibre Channel Switch, attach the AC power cord to the receptacle on the back of the switch and to the power source.

The switch runs its self-tests and begins normal operation—this may take a few minutes:

1. The switch LEDs (Input Power, Heartbeat, System Fault) illuminate followed by all port Logged-in LEDs. The Logged-in LEDs that illuminate indicate the ports that are enabled.
2. After a couple seconds the System Fault LED is extinguished while the Input Power LED and Heartbeat LED remain illuminated.
3. After approximately one minute, the POST executes and the Heartbeat LED is extinguished.
4. After about another minute, the POST is complete, all LEDs are extinguished except the Input Power LED and the Heartbeat LED:
   - The Input Power LED remains illuminated indicating that the switch logic circuitry is receiving DC voltage. If not, contact your authorized maintenance provider.
   - The Heartbeat LED indicates the results of the POST. The POST tests the condition of firmware, memories, data-paths, and switch logic circuitry. If the Heartbeat LED blinks steadily about once per second, the POST was successful, and you can continue with the installation process. Any other blink pattern indicates that an error has occurred. For more information, see "Heartbeat LED blink patterns" on page 42.

Connect the management station or workstation to the switch

You can manage the switch using the Simple SAN Connection Manager, QuickTools, or the CLI. Simple SAN Connection Manager requires at least one FC connection and an Ethernet connection to the switch. QuickTools requires an Ethernet connection to the switch. The CLI can use an Ethernet connection or a serial connection.

- If this switch is part of the 8Gb Simple SAN Connectivity Kit installation:

    a. Connect at least one FC cable from the management station to the switch, or to another switch in the same fabric.

    b. Use a 10/100 Base-T straight cable to connect the switch Ethernet port to the LAN that connects your management station that will run Simple SAN Connection Manager (see Indirect Ethernet in Figure 13).

- If this switch is a standalone installation and you plan to use QuickTools or the CLI, connect the switch Ethernet port to the workstation, in one of the following ways:

    - Indirect Ethernet connection from the workstation to the switch RJ-45 Ethernet connector through an Ethernet switch or a hub. This requires a 10/100 Base-T straight cable (Figure 13).

    - Direct Ethernet connection from the workstation to the switch RJ-45 Ethernet connector. This requires a 10/100 Base-T cross-over cable (Figure 13).

    - Serial port connection from the workstation to the switch RS-232 serial port connector. This requires a null modem F/F DB9 cable (Figure 13). This connection supports the CLI only.
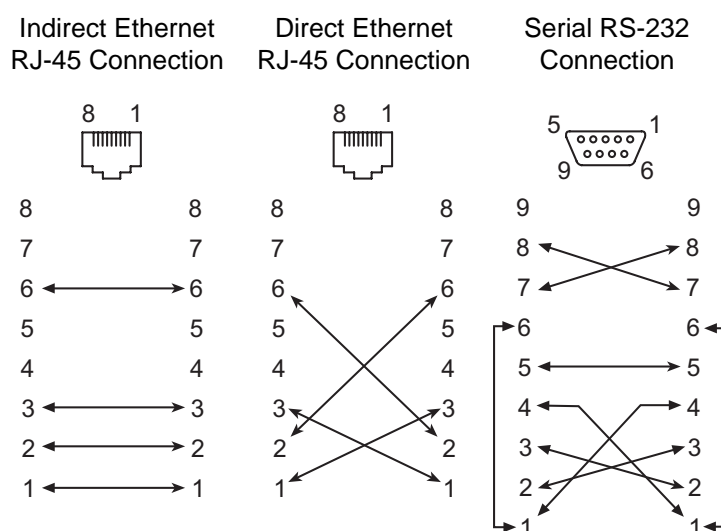
Figure 13 Management station and workstation cable connections

Configure the switch

You can configure the switch using Simple SAN Connection Manager, QuickTools, or the CLI.

Simple SAN Connection Manager switch configuration

For information about installing the Simple SAN Connection Manager application, see the *HP StorageWorks 8Gb Simple SAN Connectivity Kit quick start instructions*. The Simple SAN Connection Manager software will prompt you to set the switch IP address, administrator password, and default zoning when you first start that application.

When the configuration is complete, proceed to "Cable devices to the switch" on page 36.

QuickTools switch configuration

To log in and configure the switch using QuickTools:

1. Open an Internet browser and enter the default IP address 10.0.0.1 to start the QuickTools web applet.

2. Log in to the switch using the default user name (*admin*) and password (*password*).

3. Obtain the IP address and subnet mask from your network administrator.

4. Open the QuickTools Wizards menu and select **Configuration Wizard**. Follow the instructions to set the IP address and the password. Changing the IP address will terminate the QuickTools session.

5. Open an Internet browser again and log in with the new IP address.

6. When the configuration is complete, proceed to "Cable devices to the switch" on page 36.

CLI switch configuration

To configure the switch using the command line interface.

1. Open a command window according to the type of workstation and connection.

   For an Ethernet connection (all platforms), open a Telnet session with the default switch IP address and log in to the switch with default account name and password (admin/password).

   ```
   telnet 10.0.0.1
   Switch Login: admin
   Password:      *******
   ```

   📝 **NOTE:** To insure fabric security, you should change the password for the Admin account name. See the `passwd` command in the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*

   For a Windows serial connection, open the HyperTerminal application on a Windows platform.

   a. Click **Start**, then select **Programs>Accessories>Communications>HyperTerminal**.

   b. Select the connection you created earlier and click **OK**. See "Configuring the workstation serial port" on page 33.

   For a Linux serial connection, open a command window and enter the following command:

   ```
   minicom
   ```

2. Open an admin session and enter the `set setup system` CLI command. Enter the values you want for switch IP address (EthNetworkAddress) and the network mask (EthNetworkMask). For more information about CLI commands, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

   ```
   8/20q FC Switch #> admin start
   8/20q FC Switch (admin) #> set setup system
   ```

3. Open a Config Edit session and use the `set config switch` CLI command to modify the switch configuration.

4. When the configuration is complete, proceed to "Cable devices to the switch" on page 36.

Cable devices to the switch

Connect cables to the SFP transceivers and their corresponding devices, and then energize the devices. Device host bus adapters can have SFP (or SFF) transceivers. Duplex cable connectors are keyed to ensure proper orientation. Choose the Fibre Channel cables with the connector combination that matches the device host bus adapter.

GL_Ports self configure as FL_Ports when connected to loop of devices or F_Ports when connected to a single device. G_Ports self-configure as F_Ports when connected to a single device. Both GL_Ports and G_Ports self-configure as E_Ports when connected to another switch.

Installing firmware

The switch comes with current firmware installed. You can upgrade the firmware from the management station or workstation as new firmware becomes available using Simple SAN Connection Manager, QuickTools, or the CLI. This guide describes the use of QuickTools and the CLI. For information about installing firmware using Simple SAN Connection Manager, see the *HP StorageWorks Simple SAN Connection Manager user guide*.

- Using QuickTools to install firmware, page 37
- Using the CLI to install firmware, page 37

You can load and activate firmware upgrades on an operating switch without disrupting data traffic or re-initializing attached devices. If you attempt to perform a non-disruptive activation without satisfying the following conditions, the activation will fail. If the non-disruptive activation fails, you will usually be prompted to try again later. Otherwise, the switch will perform a disruptive activation.

- The current firmware version supports the installation and non-disruptive activation of the new firmware. For information about compatible firmware versions, see the firmware release notes.
- No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, changing switch configurations, or installing firmware.
- No port in the fabric is in the diagnostic state.
- No Zoning Edit sessions are open in the fabric.
- No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.

Install firmware on one switch at a time in the fabric. If you are installing firmware on one switch, wait 120 seconds after the activation is complete before installing firmware on a second switch.

Ports that are stable when the non-disruptive activation begins and then change states, will be reset. When the non-disruptive activation is complete, Simple SAN Connection Manager and QuickTools sessions reconnect automatically. However, Telnet sessions must be restarted manually.

☼ **TIP:** After upgrading firmware that includes changes to QuickTools, an open QuickTools session may indicate that the firmware is not supported. This means the new firmware is not supported by the previous QuickTools version. To correct this, close the QuickTools session and the browser window, then open a new QuickTools session.

Using QuickTools to install firmware

To install firmware using QuickTools:

1. In the faceplate display, open the Switch menu and select **Load Firmware**.
2. In the Firmware Upload dialog, click **Browse** to browse and select the firmware file to be uploaded.
3. Click **Start** to begin the firmware load process. You will be shown a message warning you that the switch will be reset to activate the firmware.
4. QuickTools prompts you to activate the new firmware using a hot (non-disruptive) reset, if possible. Click **OK** to reset the switch and activate the new firmware.

Using the CLI to install firmware

The method you choose to install firmware using the CLI depends on the type of firmware activation you want.

- For a disruptive activation, enter the `firmware install` or `image install` command to download the firmware image file from an FTP or TFTP server, unpack it, and activate it in one step. See "One-step firmware installation" on page 38.
- For a non-disruptive activation, enter the `image fetch` command to download the firmware image file from an FTP or TFTP server. Enter the `image unpack` command to unpack the image file, then enter the `hotreset` command to perform a non-disruptive activation. See "Custom firmware installation" on page 39.

For information about the CLI commands, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

One-step firmware installation

The `firmware install` and `image install` commands download the firmware image file from an FTP or TFTP server to the switch, unpack the image file, and perform a disruptive activation in one step. The installation process prompts you to enter the following:

- The file transfer protocol (FTP or TFTP)
- IP address of the remote host
- An account name and password on the remote host (FTP only)
- Pathname for the firmware image file

For information about the CLI commands, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide.*

1. Enter the following commands to download the firmware from a remote host to the switch, install the firmware, then reset the switch to activate the firmware.

   ```
   8/20q FC Switch #> admin start

   8/20q FC Switch #> firmware install

    The switch will be reset. This process will cause a
     disruption to I/O traffic.

    Continuing with this action will terminate all management
     sessions,including any Telnet sessions. When the firmware
     activation is complete, you may log in to the switch again.

    Do you want to continue? [y/n]: y

    Press 'q' and the ENTER key to abort this command.
   ```

2. Enter your choice for the file transfer protocol with which to download the firmware image file. FTP requires an user account and a password; TFTP does not.

   ```
   FTP or TFTP      : ftp
   ```

3. Enter your account name on the remote host (FTP only) and the IP address of the remote host. When prompted for the source file name, enter the path for the firmware image file.

   ```
   User Account     : johndoe

   IP Address       : 10.0.0.254

   Source Filename : 6.9.00.11_mpc

   About to install image.  Do you want to continue? [y/n] y
   ```

4. When prompted to install the new firmware, enter `y` to continue or `n` to cancel. Entering `y` will disrupt traffic. This is the last opportunity to cancel.

   ```
   About to install image. Do you want to continue? [y/n] y
   Connected to 10.20.20.200 (10.20.20.200).

   220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
   ```

5. Enter the password for your account name (FTP only).

   ```
   331 Password required for johndoe.
   Password:******
   230 User johndoe logged in.
   ```

The firmware will now be downloaded from the remote host to the switch, installed, and activated.

Custom firmware installation

A custom firmware installation downloads the firmware image file from an FTP or TFTP server to the switch, unpacks the image file, and resets the switch in separate steps. This allows you to choose the type of switch reset and whether the activation will be disruptive (`reset switch` command) or nondisruptive (`hotreset` command). The following example illustrates a custom firmware installation with a nondisruptive activation.

1. Download the firmware image file from the server to the switch.

   - If your server has an FTP server, you can enter the `image fetch` command:

     ```
     8/20q FC Switch (admin) #> image fetch account_name ip_address
     filename
     ```

   - If your server has a TFTP server, you can enter the `image tftp` command to download the firmware image file.

     ```
     8/20q FC Switch (admin) #> image tftp ip_address filename
     ```

   - If your server has neither an FTP nor a TFTP server, open an FTP session and enter FTP commands:

     ```
     >ftp ip_address or switchname
     user:images
     password: images
     ftp>bin
     ftp>put filename
     ftp>quit
     ```

2. Display the list of firmware image files on the switch to confirm that the file was loaded.

   ```
   8/20q FC Switch (admin) $>image list
   ```

3. Unpack the firmware image file to install the new firmware in flash memory.

   ```
   8/20q FC Switch (admin) $>image unpack filename
   ```

4. Wait for the unpack to complete.

   ```
   image unpack command result: Passed
   ```

5. A message will prompt you to reset the switch to activate the firmware. Use the `hotreset` command to attempt a non-disruptive activation.

   ```
   8/20q FC Switch (admin) $>hotreset
   ```

Adding a switch to an existing fabric

If there are no special conditions to be configured for the new switch, plug in the switch. The switch becomes functional with the default fabric configuration. The default fabric configuration settings are as follows:

- Fabric zoning is sent to the switch from the fabric.
- All ports will be GL_Ports.
- The default IP address 10.0.0.1 is assigned to the switch without a gateway or boot protocol configured: Reverse Address Resolution Protocol (RARP) Bootstrap Protocol (BOOTP), and Dynamic Host Configuration Protocol (DHCP).

If you are adding a switch to a fabric and do not want to accept the default fabric configuration:

1. If the switch is not new from the factory, reset the switch to the factory configuration before adding the switch to the fabric.
2. If you want to manage the switch through the Ethernet port, you must first configure the IP address.
3. Plug in the inter-switch links (ISL), but do not connect the devices.
4. Configure the port types for the new switch. The ports can be G_Port, GL_Port, F_Port, FL_Port, or Donor.
5. Connect the devices to the switch.
6. Make any necessary zoning changes.

Installing feature license keys

for information about available license keys, see "Feature licenses" on page 21. To install a license key using QuickTools:

1. Open the Switch Menu and select **Features** to open the Feature Licenses dialog.
2. In the Feature Licenses dialog, click **Add** to open the Add License Key dialog.
3. In the Add License Key dialog, enter the license key in the Key field.
4. Click **Get Description** to display the upgrade description.
5. Click **Add** to upgrade the switch. Allow a minute or two for the upgrade to complete.

To upgrade a switch using the command line interface, see the `feature` command in the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

4 Diagnostics and troubleshooting

Diagnostic information about the switch is available through the switch LEDs and the port LEDs. Diagnostic information is also available through the CLI, QuickTools, or Simple SAN Connection Manager event logs and error displays. This section describes the following types of diagnostics:

- Switch diagnostics, page 41 describes the Input Power LED and System Fault LED indications.
- Power-On self test diagnostics, page 42 describe the Heartbeat LED and the port Logged-in LED indications.

This section also describes using maintenance mode to recover a disabled switch.

Switch diagnostics

The 8/20q Fibre Channel Switch has three switch LEDs that are used for diagnostics: Input Power LED, Heartbeat LED, and the System Fault LED (Figure 14).
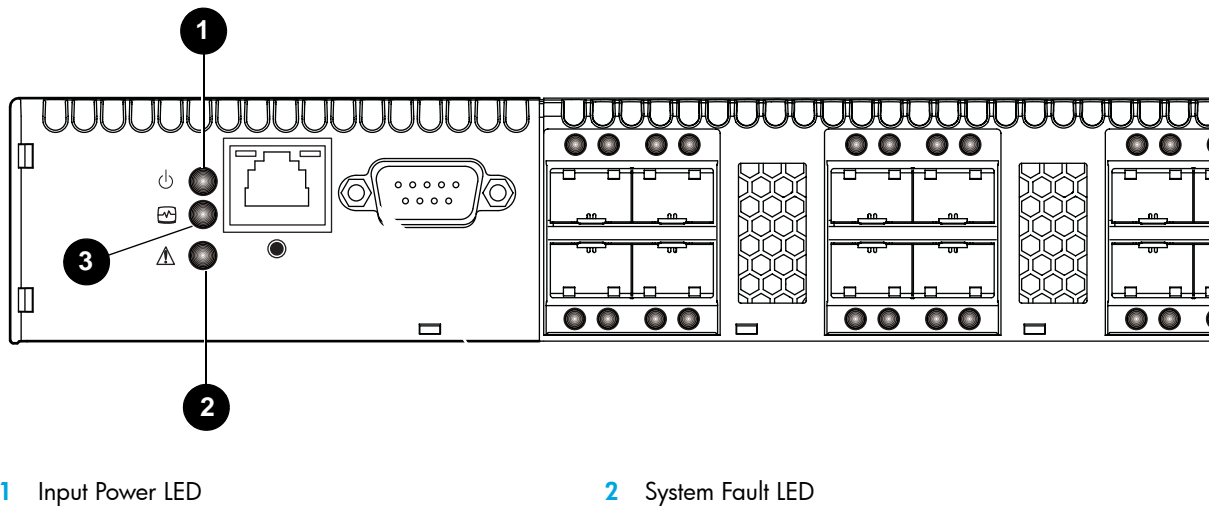
1	Input Power LED	2	System Fault LED
3	Heartbeat LED		

Figure 14 Switch LEDs

The following conditions are described in this section:

- Input power LED is extinguished, page 41
- System fault LED is illuminated, page 42

Input power LED is extinguished

The Input Power LED illuminates to indicate that the switch logic circuitry is receiving proper voltages. If the Input Power LED is extinguished:

1. Inspect the power cords and connectors. Is the cord unplugged? Is the cord or connector damaged?
   - Yes—Make necessary corrections or repairs. If the condition remains, continue.
   - No—Continue.
2. Inspect the AC power source. Is the power source delivering the proper voltage?
   - Yes—Continue.
   - No—Make necessary repairs. If the condition remains, contact your authorized maintenance provider.

System fault LED is illuminated

The System Fault LED illuminates to indicate that a fault exists in the switch firmware or hardware. If the System Fault LED illuminates, identify the Heartbeat LED error blink pattern and take the necessary actions. See "Heartbeat LED blink patterns" on page 42.

Power-On self test diagnostics

The switch performs a series of tests as part of its power-up procedure. The POST diagnostic program performs the following tests:

- Checksum tests on the boot firmware in Programmable read-only memory (PROM) and the switch firmware in flash memory
- Internal data loopback test on all ports
- Access and integrity test on the Application-specific integrated circuit (ASIC)

During the POST, the switch logs any errors encountered. Some POST errors are critical, others are not. The switch uses the Heartbeat LED and the Logged-in LED to indicate switch and port status. A critical error disables the switch so that it will not operate. A non-critical error allows the switch to operate, but disables the ports that have errors. If two or more ports fail the POST, the entire switch is disabled. Whether the problem is critical or not, contact your authorized maintenance provider.

If there are no errors, the Heartbeat LED blinks at a steady rate of once per second. If a critical error occurs, the Heartbeat LED will show a blink pattern that indicates an error, and the System Fault LED will illuminate. If there are non-critical errors, the switch disables the failed ports and flashes the associated Logged-in LEDs. For more information, see "Heartbeat LED blink patterns" on page 42.

Heartbeat LED blink patterns

The Heartbeat LED indicates the operational status of the switch. When the POST completes with no errors, the Heartbeat LED blinks at steady rate of once per second. When the switch is in maintenance mode, the Heartbeat LED illuminates continuously. For more information, see "Recovering a switch using maintenance mode" on page 46. All other blink patterns indicate critical errors. In addition to producing a Heartbeat error blink patterns, a critical error also illuminates the System Fault LED.

The Heartbeat LED shows an error blink pattern for the following conditions:

- 1 blink—Normal operation
- 2 blinks—Internal firmware failure blink pattern, page 42
- 3 blinks—Fatal POST error blink pattern, page 43
- 4 blinks—Configuration file system error blink pattern, page 43
- 5 blinks—Over-temperature blink pattern, page 43

Internal firmware failure blink pattern

An internal firmware failure blink pattern is 2 blinks followed by a two second pause. The 2-blink error pattern indicates that the firmware has failed, and that the switch must be reset. Momentarily press and release the Maintenance button to reset the switch.
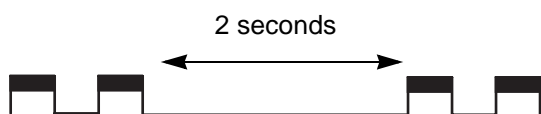
Fatal POST error blink pattern

A system error blink pattern is 3 blinks followed by a 2-second pause. The 3-blink error pattern indicates that a POST failure or a system error has left the switch inoperable. If a system error occurs, contact your authorized maintenance provider. Momentarily press and release the Maintenance button to reset the switch.
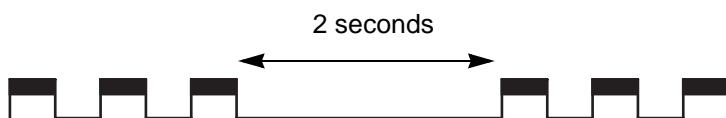
2 seconds

Configuration file system error blink pattern

A configuration file system error blink pattern is 4 blinks followed by a 2-second pause. The 4-blink error pattern indicates that a configuration file system error has occurred, and that the configuration file must be restored.

2 seconds
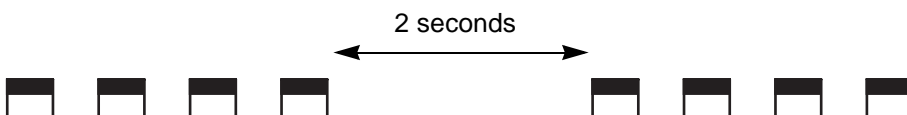
To restore the switch configuration:

1. Establish communications with the switch using Telnet. Enter one of the following on the command line:

   `telnet xxx.xxx.xxx.xxx`

   or

   `telnet switchname`

   where `xxx.xxx.xxx.xxx` is the switch IP address and *switchname* is the switch name associated with the IP address.

2. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are `admin` and `password` respectively.

3. Open an admin session to acquire the necessary authority.

   `8/20q FC Switch $> admin start`

4. Restore the configuration. When the restore is complete, the switch will reset.

   `8/20q FC Switch (admin) $> config restore`

   If a configuration does not exist, enter the `config backup` CLI command, then enter the `config restore` command.

Over-temperature blink pattern

An over-temperature blink pattern is 5 blinks followed by a 2-second pause. The 5-blink error pattern indicates that the air temperature inside the switch has exceeded the failure temperature threshold.

2 seconds
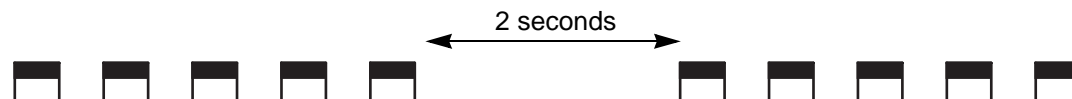
If the Heartbeat LED shows the over-temperature blink pattern:

1. Inspect the switch vents. Are the intake and exhaust vents clear?

   • Yes—Continue.

   • No—Remove any debris from fan intake and exhaust if necessary. If the condition remains, continue.

2. Consider the ambient air temperature near the switch and clearance around the switch. Make necessary corrections. If the condition remains, power down the switch and contact your authorized maintenance provider.

Logged-in LED indications

Port diagnostics are indicated by the Logged-in LED for each port (Figure 15).
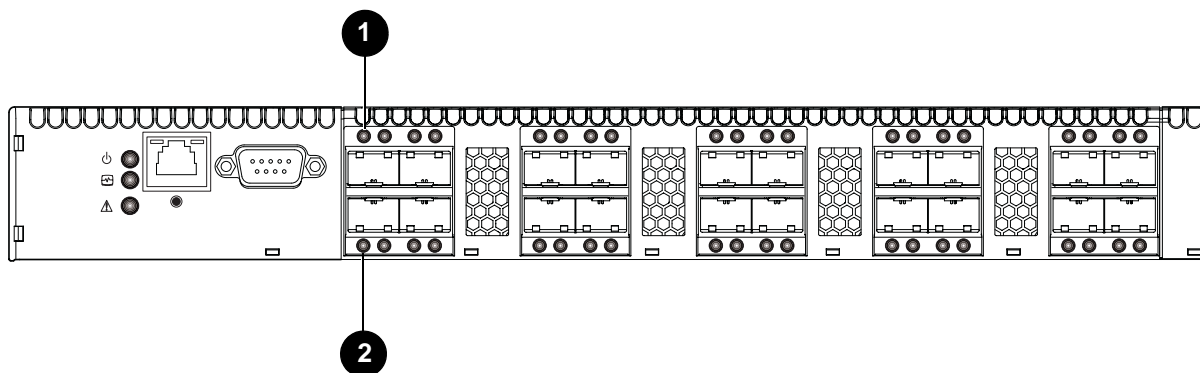
| 1 | Logged-in LED (port 0) | 2 | Logged-in LED (port 10) |

Figure 15 Logged-in LED

The Logged-in LED has three indications:

- Continuous illumination: A device is logged in to the port.
- Flashing once per second: A device is logging in to the port, or the port is in the diagnostics state.
- Flashing twice per second: The port is down, offline, or an error has occurred.

If a Logged-in LED is flashing two times per second, review the event browser for alarm messages regarding the affected port. You can also inspect the alarm log using the command line interface, `show alarm` command. If there is an error, alarm messages may point to one or more of the following conditions:

- E_Port isolation, page 44
- Excessive port errors, page 45

E_Port isolation

A Logged-in LED error indication is often the result of E_Port isolation. E_Port isolation can be caused by the following:

- Security failure
- A port configured as an F_Port or an FL_Port is connected to another switch
- Conflicting domain IDs
- Conflicting timeout values
- Conflicting zone membership between active zone sets

Using QuickTools, review the event browser, and perform the following procedure to diagnose and correct an isolated E_Port:

1. Does the QuickTools event browser show an alarm about an invalid attach on the affected port?
    - Yes—If you have configured device security, review the ISL group in the active security set to ensure that the membership includes the necessary ports and that the secrets on all switches are correct.
    - No—Continue.
2. Does the QuickTools event browser show a repeating alarm about an unsupported E_Port command on the affected port?
    - Yes—The port is configured as an FL_Port and connected to another switch. Correct the port connection or the port type.
    - No—Continue.

3. Display the fabric domain IDs using the `show domains` CLI command or by selecting the QuickTools **Switch** tab, **Summary** icon. Are all domain IDs in the fabric unique?

   • Yes—Continue.
   • No—Correct the domain IDs on the offending switches using the `set config switch` CLI command or the QuickTools Switch Properties dialog. Reset the port. If the condition remains, continue.

4. Compare the RA_TOV and ED_TOV timeout values for all switches in the fabric using the `show config switch` CLI command or by selecting the QuickTools **Switch** tab, **Advanced** icon. Is each timeout value the same on every switch?

   • Yes—Continue.
   • No—Correct the timeout values on the offending switches using the `set config switch` CLI command or selecting **Switch>Advanced Switch Properties** in QuickTools. Reset the port. If the condition remains, continue.

5. Display the active zone set on each switch using the `zoning active` CLI command or by selecting the QuickTools **Active Zoneset** tab. Compare the zone membership between the two active zone sets. Are they the same?

   • Yes—Contact your authorized maintenance provider.
   • No—Deactivate one of the active zone sets or edit the conflicting zones so that their membership is the same, then reset the port. If the condition remains, contact your authorized maintenance provider.

> **NOTE:** E_Port isolation can be caused by merging two fabrics whose active zone sets have two zones with the same name, but different membership.

Excessive port errors

The switch can monitor a set of port errors and generate alarms based on user-defined sample windows and thresholds. These port errors include the following:

• Cyclic Redundancy Check (CRC) errors
• Decode errors
• ISL connection count
• Device login errors
• Device logout errors
• Loss-of-signal errors

Port threshold alarm monitoring is disabled by default. For information about managing port threshold alarms, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

If the count for any of these errors exceeds the rising trigger for three consecutive sample windows, the switch generates an alarm and disables the affected port, changing its operational state to "down." Port errors can be caused by the following:

• Triggers are too low or the sample window is too small
• Faulty Fibre Channel port cable
• Faulty SFP
• Faulty port
• Faulty device or HBA

Review the event browser to determine if excessive port errors are responsible for disabling the port. Look for a message that mentions one of the monitored error types indicating that the port has been disabled, then perform the following procedure:

1. Examine the alarm configuration for the associated error using the `show config threshold` CLI command. See the `show config threshold` CLI command in the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*. Are the thresholds and sample window correct?
   - Yes—Continue
   - No—Correct the alarm configuration. If the condition remains, continue.

2. Reset the port, then perform an external port loopback test to validate the port and the SFP. For information about testing ports, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide* or the *HP StorageWorks 8/20q Fibre Channel Switch QuickTools switch management user guide*. Does the port pass the test?
   - Yes—Continue
   - No—Replace the SFP and repeat the test. If the port does not pass the test, contact your authorized maintenance provider. Otherwise continue.

3. Replace the Fibre Channel port cable. Is the problem corrected?
   - Yes—The procedure is complete.
   - No—Continue.

4. Inspect the device to which the affected port is connected and confirm that the device and its HBA are working properly. Make repairs and corrections as needed. If the condition remains, contact your authorized maintenance provider.

Recovering a switch using maintenance mode

A switch can become inoperable or unmanageable for the following reasons:

- Firmware becomes corrupt
- IP address is lost
- Switch configuration becomes corrupt
- Password is forgotten

In these specific cases, you can recover the switch using maintenance mode. Maintenance mode temporarily returns the switch IP address to 10.0.0.1 and provides opportunities to do the following:

To recover a switch:

1. Place the switch in maintenance mode by pressing and holding the Maintenance button with a pointed tool until only the Heartbeat LED is illuminated, and then release the button. The Heartbeat LED illuminates continuously when the switch is in maintenance mode.

2. Establish a Telnet session with the switch using the maintenance mode IP address 10.0.0.1.

3. Enter the maintenance mode account name (`prom`) and password (`prom`), and press **Enter**.

```
Switch login: prom
Password:xxxx
```

4. The maintenance menu displays several recovery options. To select a switch recovery option, press the corresponding number (displayed in option: field) on the keyboard and press **Enter**.

```
0)   Exit
1)   Image Unpack
2)   Reset Network Config
3)   Reset User Accounts to Default
4)   Copy Log Files
5)   Remove Switch Config
6)   Remake Filesystem
7)   Reset Switch
8)   Update Boot Loader
Option:
```

These options and their use are described in the following subsections.

Exiting the maintenance menu (option 0)

The **Exit** option closes the current Maintenance menu session. To log in again, enter the maintenance mode account name (prom) and password (prom). To return to normal operation, momentarily press and release the Maintenance button or power cycle the switch.

Unpacking a firmware image file in maintenance mode (option 1)

The **Image Unpack** option unpacks and installs new firmware when the current firmware has become corrupt. Before using this option, you must load the new firmware image file onto the switch. To install new firmware using this option:

1. Place the switch in maintenance mode. See the procedure for maintenance mode in "Recovering a switch using maintenance mode" on page 46.
2. Use FTP to load a new firmware image file onto the switch. See "Custom firmware installation" on page 39 for an example of how to load the image file. When the download is complete, close the FTP session.
3. Establish a Telnet session with the switch using the default IP address 10.0.0.1.

```
telnet 10.0.0.1
```

4. Enter the maintenance mode account name (prom) and password (prom), and press **Enter**.

```
Switch login: prom
Password: xxxx
```

5. Select option 1 from the maintenance menu. When prompted for a file name, enter the firmware image file name:

```
Image filename: filename
Unpacking 'filename', please wait...
Unpackage successful.
```

6. Select option **7, Reset Switch**, to reset the switch and exit maintenance mode.

Resetting the network configuration in maintenance mode (option 2)

The **Reset Network Config** option resets the network properties to the factory default values and saves them on the switch. For default network configuration values, see "Factory configuration defaults" on page 59.

Resetting user accounts in maintenance mode (option 3)

The **Reset User Accounts to Default** option restores the password for the Admin account name to the default (password) and removes all other user accounts from the switch.

Copying log files in maintenance mode (option 4)

The **Copy Log Files** option copies all log file buffers to a file on the switch named `logfile`. You can use FTP to download this file to the workstation, however, you must download `logfile` before resetting the switch. For information about downloading files from the switch, see the *HP StorageWorks 8/20q Fibre Channel Switch command line interface guide*.

Removing the switch configuration in maintenance mode (option 5)

The **Remove Switch Config** option deletes all configurations from the switch except the default configuration. This restores switch configuration parameters to the factory defaults. See "Factory configuration defaults" on page 59 for the factory default values.

Remaking the file system in maintenance mode (option 6)

The **Remake Filesystem** option resets the switch to the factory default values, including user accounts and zoning. Use this option to recreate the file system when the switch configuration becomes corrupt because of a loss of power. See "Factory configuration defaults" on page 59 for the factory default values.

📝 **NOTE:**   If you choose the **Remake Filesystem** option, you will lose all changes made to the fabric configuration that involve that switch, such as password and zoning changes. You must then restore the switch from an archived configuration or reconfigure the portions of the fabric that involve the switch.

Resetting the switch in maintenance mode (option 7)

The **Reset Switch** option closes the Telnet session, exits maintenance mode, and reboots the switch using the current switch configuration. All unpacked firmware image files that reside on the switch are deleted.

Updating the boot loader in maintenance mode (option 8)

The **Update Boot Loader** option updates the system boot loader which loads the Linux kernel into memory. Use this option only at the direction of your authorized maintenance provider.

A   Regulatory compliance and safety

Regulatory compliance

Federal Communications Commission notice for Class A equipment

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy, and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause unacceptable interference, in which case the user will be required to correct the interference at their own expense.

Cables

Connections to this device must be made with shielded cables with metallic RFI/EMI connector hoods in order to maintain compliance with FCC Rules and Regulations.

Laser device

All HP systems equipped with a laser device comply with safety standards, including International Electrotechnical Commission (IEC) 825. With specific regard to the laser, the equipment complies with laser product performance standards set by government agencies as a Class 1 laser product. The product does not emit hazardous light.

⚠ **WARNING!**

To reduce the risk of exposure to hazardous radiation:

- Do not try to open the laser device enclosure. There are no user-serviceable components inside.
- Do not operate controls, make adjustments, or perform procedures to the laser device other than those specified herein.
- Allow only HP authorized service technicians to repair the laser device.

Laser safety warning

This product uses Class 1 laser optical transceivers to communicate over the fiber optic conductors. The U.S. Department of Health and Human Services (DHHS) does not consider Class 1 lasers to be hazardous. The International Electrotechnical Commission (IEC) 825 Laser Safety Standard requires labeling in English, German, Finnish, and French stating that the product uses Class 1 lasers. Because it is impractical to label the transceivers, the following label is provided in this manual.

Certification and classification information

This product contains a laser internal to the fiber optic (FO) transceiver for connection to the Fibre Channel communications port.

In the USA, the FO transceiver is certified as a Class 1 laser product conforming to the requirements contained in the Department of Health and Human Services (DHHS) regulation 21 CFR, Subchapter J. A label on the plastic FO transceiver housing indicates the certification.

Outside the USA, the FO transceiver is certified as a Class 1 laser product conforming to the requirements contained in IEC 825–1:1993 and EN 60825–1:1994, including Amendment 11:1996 and Amendment 2:2001.

Laser product label

The optional Class 1 laser product label (Figure 16) or its equivalent may be located on the surface of the HP-supplied laser device or on the laser device installed in your product.

```
CLASS 1 LASER PRODUCT
LASER KLASSE 1
LUOKAN 1 LASERLAITE
APPAREIL A LASER DE CLASSE 1

TO IEC 825 (1984) + CENELEC HD 482 S1
```

Figure 16 Class 1 laser product label

This label indicates that the product is classified as a CLASS 1 LASER PRODUCT.

International notices and statements

Canadian notice (avis Canadien)

This equipment does not exceed Class A limits for radio emissions for digital apparatus, set out in Radio Interference Regulation of the Canadian Department of Communications. Operation in a residential area may cause unacceptable interference to radio and TV reception requiring the owner or operator to take whatever steps necessary to correct the interference.

Cet équipement ne dépasse pas les limites de Classe A d'émission de bruits radioélectriques por les appareils numériques, telles que prescrites par le Réglement sur le brouillage radioélectrique établi par le ministère des Communications du Canada. L'exploitation faite en milieu résidentiel peut entraîner le brouillage des réceptions radio et télé, ce qui obligerait le propriétaire ou l'opérateur à prendre les dispositions nécwssaires pour en éliminer les causes.

European Union regulatory notice

This product complies with the following Eurupean Union (EU) directives:

- Low Voltage Directive 2006/95/EC
- EMC Directive 2004/108/EC

Compliance with these directives implies conformity to applicable harmonized European standards (European norms), which are listed on the *EU Declaration of Conformity* issued by Hewlett-Packard for this product or product family. This compliance is indicated by the following conformity marking placed on the product:

$C\epsilon$ This marking is valid for non-telecommunications products and EU harmonized telecommunications products.	$C\epsilon$ **xxxx*** ⊘ This marking is valid for EU non-harmonized telecomunications products. *Notified body number (used only if applicable— refer to the product label)

Hewlett-Packard GmbH, HQ-TRE, Herrenberger Strasse 140, 71034 Boeblingen, Germany

Japanese notice

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準
こ基づくクラスＡ情報技術装置です。この装置を家庭環境で使用すると電波
方害を引き起こすことがあります。この場合には使用者が適切な対策を講ず
るよう要求されることがあります。

Korean notice

A급 기기 (업무용 정보통신기기)

이 기기는 업무용으로 전자파적합등록을 한 기기이오니
판매자 또는 사용자는 이 점을 주의하시기 바라며, 만약
잘못판매 또는 구입하였을 때에는 가정용으로 교환하시기
바랍니다.

Taiwan notice

警告使用者:

這是甲類的資訊產品, 在居住的環境中使用時, 可能會造成射
頻干擾, 在這種情況下, 使用者會被要求採取某些適當的對策.

B   Electrostatic discharge

This appendix provides the following information:

- How to prevent electrostatic discharge, page 53
- Grounding methods, page 53

How to prevent electrostatic discharge

To prevent damage to the system, you must follow certain precautions when setting up the system or handling parts. A discharge of static electricity from a finger or other conductor may damage system boards or other static-sensitive devices. This type of damage may reduce the life expectancy of the device.

To prevent electrostatic damage, observe the following precautions:

- Avoid hand contact by transporting and storing products in static-safe containers.
- Keep electrostatic-sensitive parts in their containers until they arrive at static-free workstations.
- Place parts on a grounded surface before removing them from their containers.
- Avoid touching pins, leads, or circuitry.
- Always make sure you are properly grounded when touching a static-sensitive component or assembly.

Grounding methods

There are several methods for grounding. Use one or more of the following methods when handling or installing electrostatic-sensitive parts:

- Use a wrist strap connected by a ground cord to a grounded workstation or chassis. Wrist straps are flexible straps with a minimum of 1 megohm ± 10 percent resistance in the ground cords. To provide proper ground, wear the strap snug against the skin.
- Use heel straps, toe straps, or boot straps at standing workstations. Wear the straps on both feet when standing on conductive floors or static-dissipating floor mats.
- Use conductive field service tools.
- Use a portable field service kit with a folding static-dissipating work mat.

If you do not have any of the suggested equipment for proper grounding, have an HP authorized reseller install the part.

NOTE: For more information on static electricity, or for assistance with product installation, contact your HP authorized reseller.

C Technical specifications

This appendix contains the specifications for the 8/20q Fibre Channel Switch. See "General description" on page 11 for the location of all connections, switches, controls, and components.

General specifications

Table 8 lists general specifications for the 8/20q Fibre Channel Switch.

Table 8 General specifications

Specification	Description
Fibre Channel protocols	FC-PH Rev. 4.3
	FC-PH-2
	FC-PH-3
	FC-AL Rev 4.6
	FC-AL-2 Rev 7.0
	FC-FLA
	FC-GS
	FC-GS-2
	FC-GS-3
	FC-FG
	FC-SW-2
	FC-Tape
	FC-VI
	Fibre Alliance MIB Version 4.0
	Fibre Channel Element MIB RFC 2837\
Fibre Channel classes of service	Classes 2 and 3
Modes of operation	Fibre Channel Classes 2 and 3, connectionless
Port types	G_Port, GL_Port, F_Port, FL_Port, E_Port
Port characteristics	All ports are auto-discovering and self-configuring.
Number of Fibre Channel ports	Available as 8-port and 16-port base models with license key upgrades to 12, 16, and 20 ports.

Table 8 General specifications (Continued)

Specification	Description
Scalability	Maximum 239 switches, depending on configuration. For the latest supported configurations, see the *SAN Design Reference Guide* available at http://www.hp.com/go/SANdesignguide.
Maximum user ports	> 475,000 ports depending on configuration. For the latest supported configurations, see the *SAN Design Reference Guide* available at http://www.hp.com/go/SANdesignguide.
Buffer credits	16 buffer credits per port, ASIC embedded memory
Media type	SFP optical transceiver
Fabric port speed	2.125, 4.250, 8.50 Gb/s
Maximum frame size	2148 bytes (2112 byte payload)
System processor	440EP PowerPc
Fabric latency (intra-switch) 2 Gb/s to 2 Gb/s	< 0.6 μsec
4 Gb/s to 4 Gb/s	< 0.3 μsec
8 Gb/s to 8 Gb/s	< 0.2 μsec
Bandwidth Point-to-point	425 MB, Full Duplex @ 2 Gb/s
	850 MB, Full Duplex @ 4 Gb/s
	1,700 MB, Full Duplex @ 8 Gb/s
Aggregate (single switch)	Up to 34 GB Full Duplex
Air flow	Front-to-back

Maintainability features

Table 9 lists maintainability features for the 8/20q Fibre Channel Switch.

Table 9 Maintainability features

Specification	Description
Diagnostics	The POST tests all functional components except SFP transceivers. Port tests include online, internal, and external tests.
User interface	LED indicators
Field replaceable units (FRUs)	None

Fabric management specifications

Table 10 lists fabric management specifications for the 8/20q Fibre Channel Switch.

Table 10 Fabric management specifications

Specification	Description
Management methods	Command Line Interface
	FTP
	GS-3 Management Server
	Simple SAN Connection Manager graphical user interface
	QuickTools web applet
	SMI-S
	SNMP
	TFTP
Maintenance connection	RS-232 connector; null modem F/F DB9 cable
Ethernet connection	RJ-45 connector; 10/100 BASE-T cable
Switch agent	Allows a network management station to obtain configuration values, traffic information, and failure data pertaining to the Fibre Channels using SNMP through the Ethernet interface.

Weight and physical dimensions

Table 11 lists physical properties for the 8/20q Fibre Channel Switch.

Table 11 Switch physical dimensions

Property	Value
Height	1U or 43.2 mm (1.70 in)
Width	432 mm (17 in)
Depth	305 mm (12.0 in)
Weight	4.08 kg (9 lb) with zero SFPs installed

Electrical specifications

Table 12 lists electrical specifications for the 8/20q Fibre Channel Switch.

Table 12 Electrical specifications

Specification	Description
Operating voltage	100 to 240 VAC; 50 to 60 Hz
Power source loading (maximum)	1 A at 120 VAC/0.5 A at 240 VAC
Heat output (maximum)	100 watts
Circuit protection	Internally fused

Environmental requirements

To ensure proper operation, the switch must not be subjected to environmental conditions beyond those for which it was tested. The ranges specified in Table 13 identify the acceptable environment for both operating and non-operating conditions.

Table 13 Environmental requirements

Condition	Acceptable range during operation	Acceptable range during non-operation
Temperature	0° to 40°C (32° to 104°F)	-40° to 70°C (-40° to 158°F)
Humidity	15% to 80%, non-condensing	5% to 90%, non-condensing
Altitude	3,048 m (10,000 feet) above sea level	15,240 m (50,000 feet) above sea level
Vibration (IEC 68-2-6)	5-500 Hz, random, 0.21 Grms, 10 minutes	5-500 Hz, random, 2.1 Grms, 10 minutes
Shock (IEC 68-2-7)	4 g, 11 ms, 20 repetitions	30 g, 292 ips, 13 msec, 3 square waves

D   Factory configuration defaults

This appendix describes the following factory configuration defaults:

Factory switch configuration

Enter the `show config switch` CLI command to display switch configuration values.

Table 14 Switch configuration defaults

Parameter	Default
AdminState	Online
BroadcastEnabled	True
InbandEnabled	True
FDMIEnabled	True
FDMIEntries	1,000
DefaultDomainID	1 (0x Hex)
DomainIDLock	False
SymbolicName	8/20q FC Switch
R_A_TOV	10000
E_D_TOV	2000
PrincipalPriority	254
ConfigDescription	Config Default
InteropMode	Standard

Factory port configuration

Enter the `show config port` CLI command to display port configuration values.

Table 15 Port configuration defaults

Parameter	Port Defaults
AdminState	Online
LinkSpeed	Auto
PortType	GL
SymbolicName	Port *n*, where *n* is the port number
ALFairness	False
DeviceScanEnabled	True
ForceOfflineRSCN	False
ARB_FF	False
InteropCredit	0
ExtCredit	0
FANEnable	True
AutoPerfTuning	True
LCFEnable	False
MFSEnable	False
MSEnable	True
NoClose	False
IOStreamGuard	Auto
VIEnable	False
PDISCPingEnable	True

Factory port threshold alarm configuration

Enter `Show Config Threshold` CLI command to display threshold alarm configuration values. If the ThresholdMonitoringEnabled parameter is disabled (False), none of the individual threshold monitoring parameter settings can be applied.

Table 16 Port threshold alarm configuration defaults

Parameter	Default
ThresholdMonitoringEnabled	False
CRCErrorsMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 25 1 10
DecodeErrorsMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 25 0 10
ISLMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 2 0 10
LoginMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 5 1 10
LogoutMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 5 1 10
LOSMonitoringEnabled • RisingTrigger • FallingTrigger • SampleWindow	True 100 5 10

Factory zoning configuration

Enter the `show config zoning` CLI command to display zoning configuration values.

Table 17 Zoning configuration defaults

Parameter	Default
MergeAutoSave	True
DefaultZone	Allow
DiscardInactive	False

Factory SNMP configuration

Enter the `show setup snmp` CLI command to display SNMP configuration values.

Table 18 SNMP configuration defaults

Parameter	Default
SNMPEnabled	True
Contact	`<syscontact undefined>`
Location	`<sysLocation undefined>`
Description	HP StorageWorks 8/20q Fibre Channel Switch
Trap [1-5] Address	Trap 1: `10.0.0.254`; Traps 2–5: `0.0.0.0`
Trap [1-5] Port	`162`
Trap [1-5] Severity	Warning
Trap [1-5] Version	2
Trap [1-5] Enabled	False
ObjectID	`1.3.6.1.4.1.3873.1.11`
AuthFailureTrap	False
ProxyEnabled	True

Factory switch services configuration

Enter the `show setup services` CLI command to display switch service configuration values.

Table 19 Services configuration defaults

Parameter	Default
TelnetEnabled	True
SSHEnabled	False
GUIMgmtEnabled	True
SSLMgmtEnabled	False
EmbeddedGUIEnabled	True
SNMPEnabled	True
NTPEnabled	False
CIMEnabled	True
FTPEnabled	True
MgmtServerEnabled	True
CallHomeEnabled	True

Factory system configuration

Enter the `Show Setup System` CLI command to display system configuration values.

Table 20 System configuration defaults

Parameter	Default
EthernetNetworkEnable	True
EthernetNetworkDiscovery	Static
EthernetNetworkIPAddress	10.0.0.1
EthernetNetworkIPMask	255.0.0.0
EthernetGatewayAddress	10.0.0.254
AdminTimeout	30 minutes
InactivityTimeout	0
LocalLogEnabled	True
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254
NTPClientEnabled	False
NTPServerAddress	10.0.0.254
EmbeddedGUIEnabled	True

Factory RADIUS configuration

Enter the `show setup radius` CLI command to display RADIUS configuration values.

Table 21 RADIUS configuration defaults

Parameter	Default
DeviceAuthOrder	Local
UserAuthOrder	Local
TotalServers	0
DeviceAuthServer	False
UserAuthServer	False
AccountingServer	False
ServerIPAddress	10.0.0.1
ServerUDPPort	1812
Timeout	2 seconds
Retries	0
SignPackets	False

Factory security configuration

Enter the show config security CLI command to display security configuration values.

Table 22 Security configuration defaults

Parameter	Default
AutoSave	True
FabricBindingEnabled	False
PortBindingEnabled	False

Factory Call Home configuration

Enter the show config callhome CLI command to display call home configuration values.

Table 23 Call Home service configuration defaults

Parameters	Default
PrimarySMTPServerAddr	0.0.0.0
PrimarySMTPServerPort	25
PrimarySMTPServerEnabled	False
SecondarySMTPServerAddr	0.0.0.0
SecondarySMTPServerPort	25
SecondarySMTPServerEnabled	False
ContactEmailAddress	nobody@localhost.localdomain
PhoneNumber	<undefined>
StreetAddress	<undefined>
FromEmailAddress	nobody@localhost.localdomain
ReplyToEmailAddress	nobody@localhost.localdomain
ThrottleDupsEnabled	True

Glossary

This glossary defines terms used in this guide or related to this product. It is not a comprehensive glossary of computer terms.

4-port Upgrade License A licensed feature that enables you to activate additional FC ports.

Active firmware The firmware image on the switch that is in use.

Active zone set The zone set that defines the current zoning for the fabric. See Zone set.

Activity LED A port LED that indicates when frames are entering or leaving the port.

Administrative state Assigned state that determines the operational state of the port or switch. There are two types of adminstrative states: the administrative state and the configured administrative state. The administrative state is the currently assigned port or switch state, such as `Online` or `Offline`. The configured administrative state is the state that is saved in the switch configuration, which determines how the switch or port comes up after a reset or power cycle.

Alarm A message generated by the switch that requires attention.

Alias A named set of ports or devices used to make defining zone set membership easier. An alias is not a zone, and it cannot have a zone or another alias as a member. See Zone.

Application-specific integrated circuit (ASIC) An integrated ciruit chip designed for a specific application, such as a transmission protocol or a computer.

Arbitrated loop A Fibre Channel topology where ports use arbitration to establish a point-to-point circuit.

Arbitrated Loop Physical Address (AL_PA) A unique one-byte value assigned during loop initialization to each NL_Port on a loop. See NL_Port.

BootP Boot strap protocol. A type of network server.

Buffer credit A measure of port buffer capacity, equal to one frame.

Challenge-Handshake Authentication Protocol (CHAP) An authentication protocol by which a device is challenged to verify its identity before being allowed to log in to a switch.

Class 2 service A service that multiplexes frames at frame boundaries to or from one or more N_Ports with acknowledgment provided. See N_Port.

Class 3 service A service that multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment. See N_Port.

Common Information Model (CIM) A switch service that provides for switch management through third-party applications that comply with the Storage Management Initiative–Specification (SMI-S).

Configuration wizard QuickTools wizard that automates the switch configuration process.

Device security A component of fabric security that provides for the authorization and authentication of devices that attach to a switch through the use of groups and security sets. See Group and Security set.

Domain ID User-defined number that identifies the switch in the fabric.

E_Port Expansion port. A Fibre Channel port that connects to another switch.

Event log Log of messages describing events that occur in the fabric.

F_Port Fabric port. A Fibre Channel switch port that supports a connection to a single server or storage device.

Fabric device management interface (FDMI) An interface by which device host bus adapters (HBAs) can be managed through the fabric.

Fabric management switch The switch through which the fabric is managed.

Fabric security	A feature that provides security for fabric users and devices, including user account security and fabric services. See Device security and Fabric services.
Fabric services	A component of fabric security that provides for the control of inband management and SNMP on a switch. See Fabric security and Simple Network Management Protocol (SNMP).
FC port	Fibre Channel port
FL_Port	Fabric loop port. A Fibre Channel switch port that supports a connection to up to 126 server or storage devices.
Flash memory	Memory on the switch that contains the switch control firmware.
Frame	Data unit consisting of start-of-frame (SOF) delimiter, header, data payload, CRC, and end-of-frame (EOF) delimiter.
Group	A list of device worldwide names that are authorized to attach to a switch. There are three group types: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS).
Heartbeat LED	A switch LED that indicates the status of the internal switch processor and the results of the Power-on self test.
Host bus adapter (HBA)	A circuit board that is installed in a server or storage device through which the device connects to the fabric.
Inband management	The ability to manage a switch through another switch over an inter-switch link.
Initiator	The device that initiates a data exchange with a target device.
In-order-delivery	A feature that requires that frames be received in the same order in which they were sent.
Input power LED	A switch LED that indicates that the switch logic circuitry is receiving proper DC voltages.
Inter-switch link (ISL)	The connection between two switches using E_Ports. See E_Port.
License key	A code associated with a separately-purchased feature that activates that feature on the switch.
Light Emitting Diode (LED)	One of several small lights that indicate the condition of the switch or a Fibre Channel port. See Heartbeat LED, Input power LED, System Fault LED, Activity LED, and Logged-in LED.
Logged-in LED	A Fibre Channel port LED that indicates the logged-in or initialization status of the connected devices.
Maintenance button	Momentary button on the switch used to reset the switch or place the switch in maintenance mode. See Maintenance mode.
Maintenance mode	Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes.
Management Information Base (MIB)	A set of guidelines and definitions for SNMP functions. See Simple Network Management Protocol (SNMP).
Management station	Workstation or server used to run Simple SAN Connection Manager.
N_Port	Node port. A Fibre Channel device port in a point-to-point or fabric connection.
Network Time Protocol (NTP)	A network protocol that enables a client to synchronize its time with a server.
NL_Port	Node loop port. A Fibre Channel device port that supports arbitrated loop protocol.
Pending firmware	The firmware image that will be activated upon the next switch reset.
Port binding	An authorization method that defines a list of device WWNs that can login to a switch port. See Worldwide Name (WWN).
Power-on self test (POST)	Diagnostics that the switch performs at start up.
Principal switch	The switch in the fabric that manages domain ID assignments. See Domain ID.
QuickTools	A browser-based switch management application that resides in the switch firmware.

Remote Authentication Dial-in Service (RADIUS)	A service that supports the remote authentication of user and device logins to a switch.
Secure shell (SSH)	A protocol that secures connections to the switch for the command line interface.
Secure socket layer (SSL)	A protocol that secures connections to the switch for QuickTools and SMI-S.
Security set	A set of up to three groups containing no more than one of each group type: ISL, Port, or MS. The active security set defines the device security for a switch. See Group.
Simple Network Management Protocol (SNMP)	An application protocol that manages and monitors network communications and functions. It also controls the Management Information Base (MIB). See Management Information Base (MIB).
Simple SAN Connection Manager (SSCM)	A management application that provides basic automated configuration and management of switches, HBAs, and storage devices.
Small form-factor pluggable (SFP)	A transceiver device, smaller than a GigaBit interface converter, that plugs into the Fibre Channel port.
Storage Management Initiative–Specification (SMI-S)	A standard that provides for the management of the switch through third-party management applications.
System Fault LED	A switch LED that indicates that a fault exists in the switch firmware or hardware.
Target	A storage device that responds to an initiator device.
User account	An object stored on a switch that consists of an account name, password, authority level, and expiration date.
User account security	A component of fabric security that provides for the administration and authentication of account names, passwords, expiration dates, and authority level.
Workstation	PC or Linux workstation that manages the switch using QuickTools or the command line interface (CLI).
Worldwide Name (WWN)	A unique 64-bit address assigned to a device by the device manufacturer.
Zone	A set of ports or devices grouped together to control the exchange of information.
Zone set	A set of zones grouped together. The active zone set defines the zoning for a fabric. See Zone.
Zoning database	The set of zone sets, zones, and aliases stored on a switch. See Alias, Zone, and Zone set.

Index